(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-56794
(P2004-56794A)
(43)公開日　平成16年2月19日(2004.2.19)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04L	9/32	H04L	9/00	675B	5B017
G06F	12/14	G06F	12/14	320A	5B085
G06F	15/00	G06F	15/00	330Z	5J104
G06F	17/60	G06F	17/60	142	
H04L	9/08	G06F	17/60	512	

審査請求 未請求　請求項の数 32　OL　（全 35 頁）　最終頁に続く

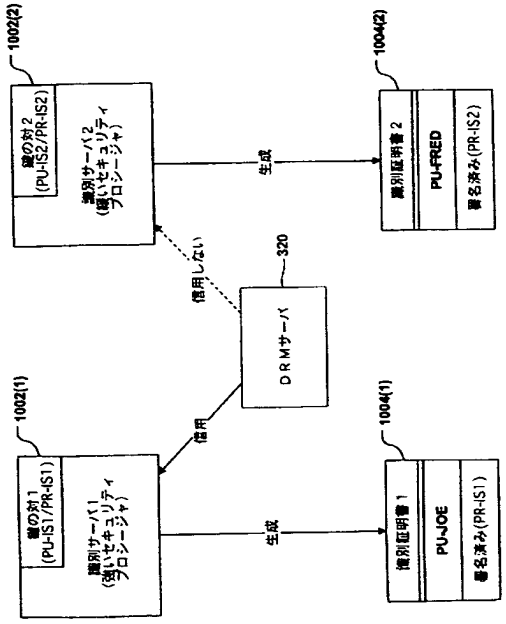
(21)出願番号　特願2003-185952(P2003-185952)
(22)出願日　平成15年6月27日(2003.6.27)
(31)優先権主張番号　10/185,077
(32)優先日　平成14年6月28日(2002.6.28)
(33)優先権主張国　米国(US)

(71)出願人　391055933
マイクロソフト　コーポレイション
ＭＩＣＲＯＳＯＦＴ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ　（番地なし）
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　アチッラ　ナリン
アメリカ合衆国　９８０１１　ワシントン州　ボズエル　ノースイースト　１４４　コート　８７４１

最終頁に続く

(54)【発明の名称】コンテンツの権利管理のための領域ベース信用モデル

(57)【要約】
【課題】システムに関与する様々なサーバ間で確立される信用関係によって、コンテンツを配布およびライセンス供与するスキームに影響を与える方法を提供する。
【解決手段】信用できる識別サーバのリストに新しい識別サーバを加えることにより、ライセンスサーバからライセンスを交付できる人々の領域を拡大する。信用される識別サーバによって交付された特定の識別証明書を除外する。
【選択図】　図１０



【特許請求の範囲】
【請求項１】
コンテンツをライセンス供与する方法であって、
ライセンス要求を受け取るステップであって、前記ライセンス要求はライセンスの交付を受けるエンティティについての識別証明書を含み、前記識別証明書は前記識別証明書を交付した交付者を示すステップと、
前記識別証明書の前記交付者を信用すると決定するステップと、
前記コンテンツを前記エンティティにライセンス供与するための条件が存在すると決定するステップと、
前記コンテンツを前記エンティティが使用するためのライセンスを生み出すステップと、
前記ライセンスを前記エンティティに送るステップと
を含むことを特徴とする方法。
【請求項２】
前記識別証明書は、（ａ）前記交付者に関連する公開鍵証明書と（ｂ）前記交付者のディジタル署名とを含み、
前記公開鍵証明書を使用して前記ディジタル署名を検証するステップをさらに含むことを特徴とする請求項１に記載の方法。
【請求項３】
前記ライセンス要求は、ライセンスを交付できるライセンス供与条件を示す権利データを含み、前記コンテンツをライセンス供与するための条件が存在すると決定する前記ステップは前記権利データに基づくことを特徴とする請求項１に記載の方法。
【請求項４】
前記識別証明書は、公開鍵を含み、前記公開鍵に対応する秘密鍵を含むかまたは前記秘密鍵に関連付けられ、ライセンスを生み出す前記ステップは、
前記公開鍵を使用して前記コンテンツのための復号鍵を暗号化して、暗号化済み復号鍵を生成するステップと、
前記暗号化済み復号鍵を前記ライセンスに含めるステップと
を含むことを特徴とする請求項１に記載の方法。
【請求項５】
前記識別証明書は、公開鍵を含み、前記公開鍵に対応する秘密鍵を含むかまたは前記秘密鍵に関連付けられ、ライセンスを生み出す前記ステップは、
対称鍵を使用して前記コンテンツのための復号鍵を暗号化して、暗号化済み復号鍵を生成するステップと、
前記対称鍵を前記公開鍵で暗号化して、暗号化済み対称鍵を生成するステップと、
前記暗号化済み対称鍵と前記暗号化済み復号鍵の両方を前記ライセンスに含めるステップと
を含むことを特徴とする請求項１に記載の方法。
【請求項６】
前記方法は信用される交付者のリストを維持するサーバによって実施され、前記識別証明書の前記交付者を信用すると決定する前記ステップは、前記交付者が前記リスト上にあるかどうかを決定するステップを含むことを特徴とする請求項１に記載の方法。
【請求項７】
前記信用される交付者はそれぞれ対応する公開鍵証明書を有し、前記リストは前記信用される交付者についての公開鍵証明書のリストを含み、
前記交付者の公開鍵証明書が前記リスト上にあるかどうかを決定するステップを含むことを特徴とする請求項６に記載の方法。
【請求項８】
前記交付者はｅメールアドレスおよびパスワードに基づいて公衆に識別証明書を交付するサーバであると決定するステップであって、前記証明書はｅメールアドレスを示すステップと、

前記ｅメールアドレスも、前記ｅメールアドレス中で識別されるドメイン名も、除外リスト上にないと決定するステップと
をさらに含むことを特徴とする請求項１に記載の方法。
【請求項９】
前記交付者に対して適用可能な除外リストが存在すると決定するステップと、
前記除外リストの条件に基づいて前記識別証明書が除外されないと決定するステップと
をさらに含むことを特徴とする請求項１に記載の方法。
【請求項１０】
前記除外リストは１つまたは複数のｅメールアドレスを含み、したがって、前記交付者によって交付された識別証明書であって前記除外リスト上のｅメールアドレスを指定する識別証明書に対しては、ライセンスは交付されない場合があり、
前記識別証明書が前記除外リスト上のｅメールアドレスを指定していないと決定するステップを含む
ことを特徴とする請求項９に記載の方法。
【請求項１１】
前記除外リストは１つまたは複数のドメイン名を含み、したがって、前記交付者によって交付された識別証明書であって前記除外リスト上のドメイン名を指定する識別証明書に対しては、ライセンスは交付されない場合があり、
前記識別証明書が前記除外リスト上のドメイン名を指定していないと決定するステップを含む
ことを特徴とする請求項９に記載の方法。
【請求項１２】
前記除外リストは１つまたは複数の識別子を含み、したがって、前記交付者によって交付された識別証明書であって前記除外リスト上の識別子を含む識別証明書に対しては、ライセンスは交付されない場合があり、
前記識別証明書が前記除外リスト上の識別子を含まないと決定するステップを含むことを特徴とする請求項９に記載の方法。
【請求項１３】
請求項１に記載の方法を実施するためのコンピュータ実行可能命令を有することを特徴とするコンピュータ可読媒体。
【請求項１４】
コンテンツをライセンス供与する方法であって、
権利ラベルを含むライセンス要求を受け取るステップを含み、前記権利ラベルは、
前記権利ラベルを交付したエンティティを示すデータと、前記エンティティに関連する秘密鍵を使用して復号可能な形の、前記コンテンツのための暗号化済み復号鍵と
を含み、方法はさらに、
前記秘密鍵が利用可能であると決定するステップと
前記秘密鍵を使用して前記暗号化済み復号鍵を復号し、それにより前記コンテンツのための復号鍵を生成するステップと、
暗号化された形の前記復号鍵を含むライセンスを生み出すステップと、
前記ライセンスをライセンス取得側に送るステップと
を含むことを特徴とする方法。
【請求項１５】
前記権利ラベルを交付する前記エンティティは関連する公開鍵証明書を有し、前記権利ラベルを交付したエンティティを示す前記データは前記公開鍵証明書を含むことを特徴とする請求項１４に記載の方法。
【請求項１６】
前記暗号化済み復号鍵は、前記権利ラベルを交付した前記エンティティに関連する公開鍵で暗号化されることを特徴とする請求項１４に記載の方法。
【請求項１７】

前記暗号化済み復号鍵は対称鍵で暗号化され、前記権利ラベルはさらに、
前記権利ラベルを交付した前記エンティティに関連する公開鍵で暗号化された前記対称鍵を含み、
前記秘密鍵を使用して前記暗号化済み復号鍵を復号する前記ステップは、
前記秘密鍵を使用して前記対称鍵を復号するステップと、
前記対称鍵を使用して前記復号鍵を復号するステップと
を含むことを特徴とする請求項１４に記載の方法。
【請求項１８】
前記権利ラベルを交付した前記エンティティが信用できると決定するステップをさらに含むことを特徴とする請求項１４に記載の方法。
【請求項１９】
前記ライセンス取得側は公開／秘密鍵の対に関連し、ライセンスを生み出す前記ステップは、
前記公開／秘密鍵の対の公開部分で前記復号鍵を暗号化するステップを含む
ことを特徴とする請求項１４に記載の方法。
【請求項２０】
前記権利ラベルに署名した前記エンティティから前記秘密鍵を受け取るステップをさらに含むことを特徴とする請求項１４に記載の方法。
【請求項２１】
前記方法を実施する前記エンティティは公開／秘密鍵の対に関連し、前記秘密鍵は、前記公開／秘密鍵の対の公開部分で暗号化された形で、前記権利ラベルに署名したエンティティから受け取られることを特徴とする請求項２０に記載の方法。
【請求項２２】
請求項１４に記載の方法を実施するためのコンピュータ実行可能命令を有することを特徴とするコンピュータ可読媒体。
【請求項２３】
コンテンツをライセンス供与するためのシステムであって、
信用されるエンティティのリストと、
ライセンス交付モジュールと
を備え、前記ライセンス交付モジュールは、ライセンスの交付を受ける識別についての識別証明書を含むライセンス要求を受け取り、前記識別証明書が前記信用されるエンティティのうちの１つによって交付されたものかどうかを決定し、前記コンテンツをライセンス供与するための条件が満たされるかどうかを決定し、前記識別証明書が前記信用されるエンティティのうちの１つによって交付されたものである場合であって前記コンテンツをライセンス供与するための条件が満たされる場合に、ライセンスを交付することを特徴とするシステム。
【請求項２４】
前記信用されるエンティティはそれぞれ、関連する公開／秘密鍵の対と、前記公開／秘密鍵の対の公開部分についての公開鍵証明書とを有し、前記信用されるエンティティのリストは、前記信用されるエンティティそれぞれについての公開鍵証明書を含むことを特徴とする請求項２３に記載のシステム。
【請求項２５】
前記識別証明書は、前記識別証明書を交付した前記信用されるエンティティのうちの１つのディジタル署名を含み、前記ライセンス交付モジュールは、前記リスト中の前記公開鍵証明書のうちの１つを使用して前記ディジタル署名を検証することを特徴とする請求項２４に記載のシステム。
【請求項２６】
前記識別証明書は、前記識別証明書を交付した前記信用されるエンティティのうちの１つについての公開鍵証明書を含み、前記ライセンス交付モジュールは、前記識別証明書中の前記公開鍵証明書を前記リスト上の前記公開鍵証明書と比較することにより、前記識別証

明書が信用されるエンティティによって交付されたものかどうかを決定することを特徴とする請求項２４に記載のシステム。
【請求項２７】
前記信用されるエンティティはそれぞれ関連する識別子を有し、前記信用されるエンティティのリストは、前記信用されるエンティティそれぞれについての識別子を含むことを特徴とする請求項２３に記載のシステム。
【請求項２８】
前記識別証明書は、前記識別証明書を交付した前記信用されるエンティティのうちの１つについての識別子を含み、前記ライセンス交付モジュールは、前記識別証明書中の前記識別子を前記リスト上の前記識別子と比較することにより、前記識別証明書が信用されるエンティティによって交付されたものかどうかを決定することを特徴とする請求項２７に記載のシステム。
【請求項２９】
前記信用されるエンティティはそれぞれ、関連する公開／秘密鍵の対と、前記公開／秘密鍵の対の公開部分についての公開鍵証明書とを有し、前記信用されるエンティティのリストは、前記信用されるエンティティそれぞれについての前記公開鍵証明書を含み、前記識別証明書はさらに、前記識別証明書を交付した前記信用されるエンティティのうちの１つについての公開鍵証明書を含み、前記ライセンス交付モジュールはさらに、前記識別証明書中の前記公開鍵証明書を前記リスト上の前記公開鍵証明書と比較することにより、前記識別証明書が信用されるエンティティによって交付されたものかどうかを決定することを特徴とする請求項２８に記載のシステム。
【請求項３０】
コンテンツをライセンス供与するためのシステムであって、前記コンテンツには、前記コンテンツのための暗号化済み復号鍵を含む権利ラベルが関連し、前記暗号化済み復号鍵は復号可能であり、
それぞれが特定の発行エンティティに関連する秘密鍵のセットと、
ライセンス交付モジュールと
を備え、前記ライセンス交付モジュールは、どの発行エンティティが前記権利ラベルを交付したかを決定し、前記権利ラベルを交付した前記発行エンティティの秘密鍵を前記秘密鍵のセットが含むかどうかを決定し、前記発行エンティティの秘密鍵を使用して前記暗号化済み復号鍵を復号して、前記コンテンツのための復号鍵を生成し、前記コンテンツのための前記復号鍵を含むライセンスを生み出すことを特徴とするシステム。
【請求項３１】
前記ライセンスは、暗号化された形で前記コンテンツのための前記復号鍵を含むことを特徴とする請求項３０に記載のシステム。
【請求項３２】
前記権利ラベルは、前記権利ラベルを交付した発行エンティティの証明書を含み、前記ライセンス交付モジュールは、前記証明書に基づいて、前記セット中のどの秘密鍵が、前記権利ラベルを交付した前記発行エンティティに対応するかを識別することを特徴とする請求項３０に記載のシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、ディジタル権利管理システムに関する。より詳細には、本発明は、権利を管理するコンテンツに対するライセンスを誰が受けることができるか、および誰がこのようなライセンスを交付することができるかを、信用モデルを使用して定義することに関する。
【０００２】
【従来の技術】
ディジタルオーディオ、ディジタルビデオ、ディジタルテキスト、ディジタルデータ、ディジタルマルチメディア、ソフトウェアなどのディジタルコンテンツを１人または複数の

ユーザに配布する場合、このようなディジタルコンテンツに関してはディジタル権利管理（「ＤＲＭ」）および施行が非常に望ましい。ディジタルコンテンツは、例えばテキスト文書などのように静的なこともあり、ライブイベントのストリーミングオーディオ／ビデオなどのようにストリーミングされることもある。権利管理システムの典型的な使用法では、ユーザがネットワーク（例えばインターネット）を介して、または物理媒体上で（例えばディスク上で）、ディジタルコンテンツを受け取る。さらに、ユーザがコンテンツを「消費」すること（例えばオーディオまたはビデオコンテンツの再生、テキストコンテンツの閲覧、ソフトウェアの実行など）が許可される場合、ユーザはこのようなコンテンツに対するライセンスも受ける。権利管理システムは、ライセンスの条件によってこのような消費が許可されるときだけユーザがコンテンツを消費できるという要件を施行する。

【０００３】

権利管理システムは通常、少なくとも２つのコンテキストで暗号に依存する。第１に、保護する必要のあるコンテンツが暗号化される。第２に、暗号化されたコンテンツを有意に使用するために復号鍵が必要な場合、鍵は信用されるエンティティだけに配布しなければならず、この信用は暗号証明書および署名を使用して確立される。最も単純な権利管理システムでは、暗号化されたコンテンツの所有者が、このコンテンツの消費者の信用性を直接に検証し、所有者が消費者の信頼性を確信すれば、復号鍵を含むライセンスをこの消費者に配布する。しかし、このようなシステムは、大きな商業的意義を有するまでに十分豊富な機能は提供しない。ほとんどのコンテンツは、商業における他のどんなものもそうであるように、複雑な関係のチェイン（連鎖）またウェブを介して配布される。例えば、コンテンツ所有者は、コンテンツに対するライセンス（したがって鍵）を交付する作業を実際にはディストリビュータに委任する場合がある。この場合、コンテンツ所有者とライセンスディストリビュータとを分離することにより、コンテンツをどのように配布するかに関してより大きなフレキシビリティがもたらされる（例えばコンテンツ所有者は、コンテンツを配布しライセンス供与サーバを運営することに時間または金銭を費やす必要がない）。一方、この分離はまた、コンテンツ所有者（コンテンツの所有権を有する）がライセンスディストリビュータ（所有者の所有権に影響力を有する）を信用することを必要とする。

【０００４】

配布／権利管理プロセスの他の面も分離することができる。例えば、ライセンス供与側は、特定のハードウェアプラットフォーム上でコンテンツを消費することをユーザに許可するライセンスを交付する場合、（ａ）ユーザの識別（ライセンス供与が特定のユーザに限定される場合）と、（ｂ）コンテンツが消費されることになるプラットフォームのセキュリティとについて暗黙的に決定を行っている。ライセンス供与側がこの決定を直接行うこともできるが、別のエンティティ（「識別交付者」または「識別サーバ」）がこのような識別とプラットフォームセキュリティとを証明する証明書を交付するようにして、ライセンス供与側は単にこの証明書に依存するようにすることが有用な場合もある。しかし、継続的なコンテンツ制御は、詐称者または安全でないプラットフォームに対して交付しないという証明書に依存するので、この分離は、ライセンス供与側が識別証明書の交付者を信用することを暗黙的に必要とする。配布および権利管理プロセスにおいて分離することのできる他の形態は、ライセンスを交付できる状況を定義するエンティティが、ライセンスを実際に交付するエンティティとは異なる場合である。したがって、コンテンツを発行する場合、第１のエンティティが、ライセンス供与条件を指定する権利ラベルにディジタル署名し、第２のエンティティが、コンテンツの使用を許可するライセンスを実際に交付することができる。このタイプの分離もやはり、第１のエンティティが、指定の条件下でのみライセンスを交付するよう第２のエンティティを信用することを必要とする。

【０００５】

【発明が解決しようとする課題】

以上の考察から、誰がどんな状況下で文書をライセンス供与できるかに関する実際的現実は、誰が誰を信用するかに影響される可能性があることが理解できる。誰がコンテンツに

対するライセンスを得ることができるかについての領域は、配布およびライセンス供与プロセスに関与する様々なサーバ間で信用を広げる（または抑える）ことによって拡張（または収縮）させることができる。

【０００６】

本発明は、従来技術で実現されていない、信用を用いてコンテンツへのアクセスを制御する技法を提供する。

【０００７】

本発明は、信用モデルを使用して、権利管理されるコンテンツがどのように、またどんな状況でライセンス供与されるかに影響を与えるシステムおよび方法を提供することを目的とする。

【０００８】

【課題を解決するための手段】

本発明によるディジタル権利管理（ＤＲＭ）システムは、コンテンツのライセンス供与を受けるエンティティのみがコンテンツを使用できるような形でコンテンツを発行する。ＤＲＭ保護されるコンテンツは、暗号化され、次いで「署名済み権利ラベル」付きで発行される。署名済み権利ラベルは、とりわけ（ａ）コンテンツをどのように使用することができ、誰にライセンス供与することができるかを定義する権利データ、（ｂ）権利ラベルを交付したサーバの公開鍵によって（直接的または間接的に）暗号化された、コンテンツのための復号鍵、および（ｃ）権利ラベルを交付したサーバのディジタル署名を含む。権利管理されるコンテンツを受け取る可能性を有する各エンティティ（例えば個人、会社部門、非営利団体など）は、そのエンティティの識別を定義する「エンティティ証明書」を取得する。エンティティ証明書は（ａ）公開／秘密鍵の対、および（ｂ）エンティティ証明書を交付したサーバの署名を含む。

【０００９】

コンテンツをライセンス供与するよう求める要求は、コンテンツについての署名済み権利ラベルと、ライセンスの交付を受けるエンティティのエンティティ証明書とを含む。ＤＲＭライセンスサーバがこのような要求を受け取ると、ＤＲＭライセンスサーバは、ライセンス供与側が信用するサーバによってこのエンティティ証明書が署名されたことを決定する。（ライセンス供与側は例えば、サーバがこのような証明書を交付する前にエンティティの識別を十分厳格に検証することを、確認したい場合もある。）ライセンスサーバがエンティティ証明書の署名者を信用する場合、ライセンスサーバは、権利ラベルに署名したエンティティに代わってライセンスを交付できるかどうかを決定する。一般にライセンスサーバは、（ａ）サーバ自体が交付した権利ラベルと、（ｂ）秘密鍵をライセンスサーバと共有していた他のＤＲＭサーバとに基づいて、ライセンスを交付することができる。（権利ラベルは交付者サーバの公開鍵で暗号化されたコンテンツ復号鍵を含むので、ライセンスサーバは、権利ラベルを交付したサーバの秘密鍵を必要とする。ライセンスはエンティティ証明書の公開鍵で暗号化されたコンテンツ復号鍵を含むので、ライセンスサーバは、コンテンツ鍵をエンティティ証明書の公開鍵で再暗号化できるように、コンテンツ鍵を復号するための適用可能な秘密鍵を必要とする。）

ＤＲＭサーバのオペレータは、他のどのサーバが信用され、どのサーバが信用されないかを決定することにより、コンテンツをライセンス供与できる人々の領域を拡大（または縮小）することができ、さもなければ配布スキームのトポロジに影響を与えることができる。これらの決定は、様々な例示的な信用モデルとの関連で用いることができる。

【００１０】

第１の例では、信用決定を利用して「信用ペルソナ領域」を実装することができ、ＤＲＭサーバが、エンティティ証明書を交付するものとして信用されるサーバのリストを維持する。このスキームは、２つの組織が、権利管理される情報をそれらのメンバによって共有できるようにしたい場合に有用である。したがって、会社Ａおよび会社Ｂがそれぞれ自社の従業員についてのエンティティ証明書を交付する場合、これらの会社は、相互の識別サーバを信用することに同意する。これにより、会社Ａの従業員は、会社Ｂの従業員にライ

センス供与可能なコンテンツを発行することができ、その逆も可能である。会社Ａの従業員によって発行されたコンテンツを受け取る会社Ｂの従業員は、権利ラベルおよび自分のエンティティ証明書を会社ＡのＤＲＭライセンスサーバに提示する。２つの会社は相互の識別サーバを信用することに同意しているので、このライセンスサーバは、会社Ｂの従業員のエンティティ証明書に対してコンテンツをライセンス供与することができる。この例の一変形は、ＤＲＭライセンスサーバが、ｅメールアドレスに基づく公用の識別サーバ（ＭＩＣＲＯＳＯＦＴ．ＮＥＴ ＰＡＳＳＰＯＲＴサーバなど）を一般に信用し、例外として、このようなサーバが特定のペルソナ（例えばｊｏｅ@ｕｎｔｒａｃｅａｂｌｅａｄｄｒｅＳＳ．ｃｏｍ）またはドメイン（例えばｕｎｔｒａｃｅａｂｌｅａｄｄｒｅＳＳ．ｃｏｍからのすべてのアドレス）に交付した証明書は除くものである。さらにより一般的には、信用ペルソナ領域にある任意の識別サーバについて、ｅメールアドレス、ドメイン、または他の何らかの識別子に基づく除外リストを生み出すことができ、それによりライセンスサーバは、識別サーバを一般に信用すると共に、その信用に対する特定の例外を切り出すことができる。

【００１１】

第２の例では、信用決定を利用して「信用文書領域」を実装することができる。この場合、第１のＤＲＭサーバが、第２のＤＲＭサーバによって生み出された権利ラベルに基づいて、第２のＤＲＭサーバの秘密鍵を得ることによってライセンスを交付することができる。実際このようなトランザクションは、第２のＤＲＭサーバが、第２のサーバの代わりにライセンスを交付するものとして第１のＤＲＭサーバを信用することを意味する。このスキームは、会社内の２つの部門がそれぞれＤＲＭサーバを維持する場合（例えば２つの部門が地理的に離れている場合）に有用である。この場合、各部門は、他方の部門がそれ自体のＤＲＭサーバ上でライセンス供与することのできるコンテンツを発行したいことがある。例えば、部門Ａの従業員が部門ＡのＤＲＭサーバを使用してコンテンツを発行し、発行したコンテンツを署名済み権利ラベルと共に部門Ｂの従業員に送る。次いで、部門Ｂの従業員は、ライセンスを求めて署名済み権利ラベルを部門ＢのＤＲＭサーバにサブミットする。このシナリオは、部門Ａの秘密鍵を部門ＢのＤＲＭサーバに提供することによって可能にすることができる。

【００１２】

本発明のその他の特徴については以下に説明する。

【００１３】

以上の概要、ならびに後続の好適実施形態の詳細な説明は、添付の図面と共に読めばよりよく理解される。図面には、本発明を例示するために本発明の例示的な構造を示す。ただし本発明は、開示する特定の方法および手段に限定されるものではない。

【００１４】

【発明の実施の形態】

例示的なコンピューティング環境

図１および後続の考察に、本発明を実施することのできる適したコンピューティング環境の簡単な一般的記述を提供する。ただし、ハンドヘルド、ポータブル、およびその他あらゆる種類のコンピューティングデバイスが、本発明に関連した使用に企図されることを理解されたい。以下では汎用コンピュータについて説明するが、これは一例に過ぎず、本発明は、ネットワークサーバ相互運用性および対話を有するシンクライアントだけを必要とする。したがって本発明は、極めて少ないまたは最小限のクライアントリソースが関係する、ネットワークによってホストされるサービスの環境で実施することができる。例えば、クライアントデバイスが単にワールドワイドウェブに対するブラウザまたはインタフェースとして機能するだけのネットワーク化環境でも実施することができる。

【００１５】

必須ではないが本発明は、開発者が使用するためのアプリケーションプログラミングインタフェース（ＡＰＩ）を介して実施することができ、および／または、ネットワーク閲覧ソフトウェアに含めることができる。これらについて、クライアントワークステーション

、サーバ、その他のデバイスなど、１つまたは複数のコンピュータによって実行されるプログラムモジュールなどのコンピュータ実行可能命令の一般的なコンテキストで説明する。一般にプログラムモジュールは、特定のタスクを実施するか特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造などを含む。通常、プログラムモジュールの機能は、様々な実施形態で望むように組み合わせるか分散させることができる。さらに、本発明は他のコンピュータシステム構成で実施することもできることは、当業者なら理解するであろう。本発明と共に使用するのに適する他の周知のコンピューティングシステム、環境、および／または構成には、限定しないがパーソナルコンピュータ（ＰＣ）、現金自動預け払い機、サーバコンピュータ、ハンドヘルドデバイスまたはラップトップデバイス、マルチプロセッサシステム、マイクロプロセッサベースのシステム、プログラム可能な民生用電子機器、ネットワークＰＣ、ミニコンピュータ、メインフレームコンピュータなどが含まれる。本発明はまた、通信ネットワークまたはその他のデータ伝送媒体を介してリンクされたリモート処理デバイスによってタスクが実施される分散コンピューティング環境で実施することもできる。分散コンピューティング環境では、プログラムモジュールは、メモリ記憶デバイスを含めたローカルとリモートの両方のコンピュータ記憶媒体に位置することができる。

【００１６】

したがって図１に、本発明を実施することのできる適したコンピューティングシステム環境１００の例を示す。ただし先に明確にしたように、コンピューティングシステム環境１００は、適したコンピューティング環境の一例に過ぎず、本発明の使用または機能の範囲についてどんな制限を意味するものでもない。またコンピューティング環境１００は、この例示的な動作環境１００に示すコンポーネントのいずれか１つまたは組合せに関してどんな依存も要件も有するものと解釈すべきではない。

【００１７】

図１を参照すると、本発明を実施するための例示的なシステムは、コンピュータ１１０の形をとる汎用コンピューティングデバイスを含む。コンピュータ１１０のコンポーネントには、限定しないが処理ユニット１２０と、システムメモリ１３０と、システムメモリを含めた様々なシステムコンポーネントを処理ユニット１２０に結合するシステムバス１２１とを含めることができる。システムバス１２１は、様々なバスアーキテクチャのいずれかを用いた、メモリバスまたはメモリコントローラ、周辺バス、ローカルバスを含めて、いくつかのタイプのバス構造のいずれかとすることができる。限定ではなく例として、このようなアーキテクチャには、ＩＳＡ（Ｉｎｄｕｓｔｒｙ Ｓｔａｎｄａｒｄ Ａｒｃｈｉｔｅｃｔｕｒｅ）バス、ＭＣＡ（Ｍｉｃｒｏ Ｃｈａｎｎｅｌ Ａｒｃｈｉｔｅｃｔｕｒｅ）バス、ＥＩＳＡ（Ｅｎｈａｎｃｅｄ ＩＳＡ）バス、ＶＥＳＡ（Ｖｉｄｅｏ Ｅｌｅｃｔｒｏｎｉｃｓ Ｓｔａｎｄａｒｄｓ Ａｓｓｏｃｉａｔｉｏｎ）ローカルバス、およびＰＣＩ（Ｐｅｒｉｐｈｅｒａｌ ＣｏｍＰｏｎｅｎｔ Ｉｎｔｅｒｃｏｎｎｅｃｔ）バス（メザニンバスとも呼ばれる）が含まれる。

【００１８】

コンピュータ１１０は通常、様々なコンピュータ可読媒体を備える。コンピュータ可読媒体は、コンピュータ１１０からアクセスできる任意の利用可能な媒体とすることができ、揮発性と不揮発性、取外し可能と取外し不可能の両方の媒体が含まれる。限定ではなく例として、コンピュータ可読媒体には、コンピュータ記憶媒体および通信媒体を含めることができる。コンピュータ記憶媒体には、コンピュータ可読命令、データ構造、プログラムモジュール、その他のデータなどの情報を記憶するための任意の方法または技術で実現される、揮発性と不揮発性、取外し可能と取外し不可能の両方の媒体が含まれる。コンピュータ記憶媒体には、限定しないがＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリまたは他のメモリ技術、ＣＤ－ＲＯＭ、ディジタル多用途ディスク（ＤＶＤ）または他の光ディスク記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置または他の磁気記憶デバイスが含まれ、あるいは、所望の情報を記憶するのに使用できコンピュータ１１０からアクセスできるその他の任意の媒体が含まれる。通信媒体は通常、搬送波やその他のト

ランスポート機構など変調されたデータ信号中に、コンピュータ可読命令、データ構造、プログラムモジュール、またはその他のデータを組み入れたものであり、任意の情報送達媒体が含まれる。「変調されたデータ信号」という語は、信号中の情報が符号化される形で１つまたは複数の特性が設定されたまたは変更された信号を意味する。限定ではなく例として、通信媒体には、配線式ネットワークや直接配線式接続などの配線式媒体と、音響、無線周波、赤外線、その他の無線媒体などの無線媒体とが含まれる。以上の任意の組合せもコンピュータ可読媒体の範囲に含めるべきである。

【００１９】

システムメモリ１３０は、読出し専用メモリ（ＲＯＭ）１３１やランダムアクセスメモリ（ＲＡＭ）１３２など、揮発性および／または不揮発性メモリの形のコンピュータ記憶媒体を含む。ＲＯＭ１３１には通常、起動中などにコンピュータ１１０内の要素間で情報を転送するのに役立つ基本ルーチンを含むＢＩＯＳ（ｂａＳｉｃ　ｉｎＰｕｔ／ｏｕｔＰｕｔ　ＳＹＳｔｅｍ）１３３が記憶されている。ＲＡＭ１３２は通常、処理ユニット１２０がすぐにアクセス可能な、および／または処理ユニット１２０が現在作用している、データおよび／またはプログラムモジュールを含む。限定ではなく例として、図１には、オペレーティングシステム１３４、アプリケーションプログラム１３５、その他のプログラムモジュール１３６、およびプログラムデータ１３７を示す。

【００２０】

コンピュータ１１０は、その他の取外し可能／取外し不可能、揮発性／不揮発性コンピュータ記憶媒体を備えることもできる。例に過ぎないが図１には、取外し不可能および不揮発性の磁気媒体に対して読み書きするハードディスクドライブ１４１と、取外し可能および不揮発性の磁気ディスク１５２に対して読み書きする磁気ディスクドライブ１５１と、ＣＤ－ＲＯＭや他の光媒体など取外し可能および不揮発性の光ディスク１５６に対して読み書きする光ディスクドライブ１５５を示す。この例示的な動作環境で使用できる他の取外し可能／取外し不可能、揮発性／不揮発性コンピュータ記憶媒体には、限定しないが磁気テープカセット、フラッシュメモリカード、ディジタル多用途ディスク、ディジタルビデオテープ、固体ＲＡＭ、固体ＲＯＭなどが含まれる。ハードディスクドライブ１４１は通常、インタフェース１４０などの取外し可能なメモリインタフェースを介してシステムバス１２１に接続され、磁気ディスクドライブ１５１および光ディスクドライブ１５５は通常、インタフェース１５０などの取外し可能メモリインタフェースでシステムバス１２１に接続される。

【００２１】

上述の図１に示した各ドライブおよびそれらに関連するコンピュータ記憶媒体は、コンピュータ可読命令、データ構造、プログラムモジュール、およびその他のデータの記憶域をコンピュータ１１０に提供する。例えば図１には、ハードディスクドライブ１４１がオペレーティングシステム１４４、アプリケーションプログラム１４５、その他のプログラムモジュール１４６、およびプログラムデータ１４７を記憶しているのが示されている。これらのコンポーネントは、オペレーティングシステム１３４、アプリケーションプログラム１３５、その他のプログラムモジュール１３６、およびプログラムデータ１３７と同じものとすることもでき、異なるものとすることもできることに留意されたい。ここでは、オペレーティングシステム１４４、アプリケーションプログラム１４５、その他のプログラムモジュール１４６、およびプログラムデータ１４７が少なくとも異なるコピーであることを示すために、異なる番号を付してある。ユーザは、キーボード１６２や、マウス、トラックボール、またはタッチパッドと一般に呼ばれるポインティングデバイス１６１などの入力デバイスを介して、コンピュータ１１０にコマンドおよび情報を入力することができる。その他の入力デバイス（図示せず）には、マイクロホン、ジョイスティック、ゲームパッド、衛星受信アンテナ、スキャナなどを含めることができる。これらおよび他の入力デバイスは、システムバス１２１に結合されたユーザ入力インタフェース１６０を介して処理ユニット１２０に接続されることが多いが、パラレルポート、ゲームポート、ユニバーサルシリアルバス（「ＵＳＢ」）など、他のインタフェースおよびバス構造で接続

されてもよい。

【００２２】

モニタ１９１または他のタイプの表示デバイスもまた、ビデオインタフェース１９０などのインタフェースを介してシステムバス１２１に接続される。ノースブリッジなどのグラフィックスインタフェース１８２をシステムバス１２１に接続することもできる。ノースブリッジは、ＣＰＵまたはホスト処理ユニット１２０と通信し、ＡＧＰ（ａｃｃｅｌｅｒａｔｅｄ　ｇｒａＰｈｉｃｓ　Ｐｏｒｔ）通信に対する役割を担うチップセットである。１つまたは複数のグラフィックス処理ユニット（ＧＰＵ）１８４が、グラフィックスインタフェース１８２と通信することができる。なお、ＧＰＵ１８４は、一般にレジスタ記憶域などのオンチップメモリ記憶域を含み、ビデオメモリ１８６と通信する。ただし、ＧＰＵ１８４はコプロセッサの一例に過ぎず、したがって様々なコプロセッシングデバイスをコンピュータ１１０に含めることができる。モニタ１９１または他のタイプの表示デバイスもまた、ビデオインタフェース１９０などのインタフェースを介してシステムバス１２１に接続され、ビデオインタフェース１９０はビデオメモリ１８６と通信することができる。モニタ１９１に加えて、コンピュータは通常、スピーカ１９７やプリンタ１９６など他の周辺出力デバイスも備えることができ、これらは出力周辺インタフェース１９５を介して接続することができる。

【００２３】

コンピュータ１１０は、リモートコンピュータ１８０など１つまたは複数のリモートコンピュータへの論理接続を用いて、ネットワーク化された環境で動作することができる。リモートコンピュータ１８０は、パーソナルコンピュータ、サーバ、ルータ、ネットワークＰＣ、ピアデバイス、または他の一般的なネットワークノードとすることができ、図１にはメモリ記憶デバイス１８１しか示していないが、通常はコンピュータ１１０に関して上述した要素の多くまたはすべてを備える。図１に示す論理接続は、ローカルエリアネットワーク（ＬＡＮ）１７１およびワイドエリアネットワーク（ＷＡＮ）１７３を含むが、他のネットワークを含むこともできる。このようなネットワーキング環境は、オフィス、企業全体のコンピュータネットワーク、イントラネット、およびインターネットでよくみられるものである。

【００２４】

コンピュータ１１０は、ＬＡＮネットワーキング環境で使用される場合、ネットワークインタフェースまたはアダプタ１７０を介してＬＡＮ１７１に接続される。ＷＡＮネットワーキング環境で使用される場合は通常、インターネットなどのＷＡＮ１７３を介した通信を確立するためのモデム１７２または他の手段を備える。モデム１７２は内蔵でも外付けでもよく、ユーザ入力インタフェース１６０または他の適切な機構を介してシステムバス１２１に接続することができる。ネットワーク化環境では、コンピュータ１１０に関して示したプログラムモジュールまたはその一部をリモートのメモリ記憶デバイスに記憶することができる。限定ではなく例として、図１には、リモートアプリケーションプログラム１８５がメモリデバイス１８１上にあるものとして示す。図示のネットワーク接続は例示的なものであり、コンピュータ間に通信リンクを確立する他の手段を使用することもできることは理解されるであろう。

【００２５】

ディジタルコンテンツの発行

図２は、ディジタルコンテンツを発行するための、本発明によるシステムおよび方法の好適実施形態の機能ブロック図である。本明細書において「発行」という語は、信用されるエンティティがこのコンテンツに対して交付できる権利および条件のセット、ならびにこれらの権利および条件を交付できる対象を、信用されるエンティティによって確立するために、アプリケーションまたはサービスが従うプロセスを指す。本発明によれば、発行プロセスは、ディジタルコンテンツを暗号化し、可能性あるすべてのコンテンツユーザに向けてコンテンツの作者が意図した永続的および施行可能な権利のリストを関連付けることを含む。このプロセスは、コンテンツの作者が意図しない限りどんな権利またはコンテン

ツへのアクセスも禁じるように安全な方法で実施することができる。

【００２６】

本発明の好適な実施形態では、特に３つのエンティティを利用して安全なディジタルコンテンツを発行することができる。すなわち、クライアント３００上で実行され、発行に向けてコンテンツを作成するコンテンツ作成アプリケーション３０２と、やはりクライアントデバイス３００上にあるディジタル権利管理（ＤＲＭ）アプリケーションプログラムインタフェース（ＡＰＩ）３０６と、通信ネットワーク３３０を介してクライアント３００と通信可能に結合されたＤＲＭサーバ３２０である。本発明の好適な実施形態では、通信ネットワーク３３０にはインターネットが含まれるが、通信ネットワーク３３０は、例えばプロプライエタリイントラネットなど、任意のローカルまたはワイドエリアネットワークとすることができることを理解されたい。

【００２７】

コンテンツ作成アプリケーション３０２は、ディジタルコンテンツを生成する任意のアプリケーションとすることができる。例えばアプリケーション３０２は、ワードプロセッサとすることができ、あるいは、ディジタルテキストファイル、ディジタル音楽、ビデオ、または他のそのようなコンテンツを生成するその他の発行側とすることができる。コンテンツには、例えばライブイベントまたはテープに記録されたイベントのストリーミングオーディオ／ビデオなど、ストリーミングコンテンツを含めることもできる。本発明によれば、コンテンツ作成アプリケーションは、そのユーザに、ユーザの提供する鍵（ＣＫ）を使用してコンテンツを暗号化するよう促す。アプリケーション３０２は、この鍵を使用してディジタルコンテンツを暗号化し、それにより暗号化済みディジタルコンテンツファイル３０４を形成する。クライアントアプリケーションはまた、ディジタルコンテンツファイル３０４に対する権利を提供するようユーザに促す。権利データは、ディジタルコンテンツにおける権利を有する各エンティティの識別を含む。このようなエンティティは、例えば、個人、ある部類の複数の個人、またはデバイスとすることができる。このような各エンティティについて、権利データはまた、コンテンツにおいてそのエンティティが有する権利、およびこれらの権利のいずれかまたはすべてに課すことのできる条件のリストも含む。このような権利には、ディジタルコンテンツの読出し、編集、コピー、印刷などの権利を含めることができる。さらに、権利は包含的とすることも排他的とすることもできる。包含的な権利は、指定のユーザがコンテンツにおいて指定の権利を有することを示す（例えばこのユーザはディジタルコンテンツを編集することができる）。排他的な権利は、指定のユーザがコンテンツにおいて指定の権利を除くすべての権利を有することを示す（例えばこのユーザは、コピーすることを除いては、ディジタルコンテンツで何をしてもよい）。

【００２８】

本発明の一実施形態によれば、クライアントＡＰＩ３０６は、暗号化済みディジタルコンテンツおよび権利データをＤＲＭサーバ３２０に渡すことができる。ＤＲＭサーバ３２０は、以下に詳細に説明するプロセスを用いて、ユーザから譲渡された権利を施行することができるかどうかを決定し、施行することができる場合は、権利データに署名して、署名済み権利ラベル（ＳＲＬ）３０８を形成する。ただし一般には、信用される任意のエンティティが、好ましくはＤＲＭサーバ３２０によって信用される鍵を使用して、権利データに署名することができる。例えば、クライアントが、ＤＲＭサーバ３２０から提供された鍵を使用して権利データに署名することができる。

【００２９】

権利ラベル３０８は、権利記述と、暗号化済みコンテンツ鍵と、権利記述および暗号化済みコンテンツ鍵に対するディジタル署名とを表すデータを含むことができる。ＤＲＭサーバが権利ラベルに署名していれば、ＤＲＭサーバは、クライアントＡＰＩ３０６を介して署名済み権利ラベル３０８をクライアントに返し、クライアントは、署名済み権利ラベル３０８をクライアントデバイス３００上に記憶する。次いで、コンテンツ作成アプリケーション３０２は、署名済み権利ラベル３０８を暗号化済みディジタルコンテンツファイル

３０４と関連付ける。例えば、ＳＲＬ３０８を暗号化済みディジタルコンテンツファイルと連結して、権利管理されるコンテンツファイル３１０を形成することができる。ただし一般に、権利データはディジタルコンテンツと結合しなくてもよい。例えば、権利データを既知の位置に記憶し、記憶した権利データへの参照を暗号化済みディジタルコンテンツと結合してもよい。この参照は、この権利データがどこに記憶されているかを示す識別子（例えばこの権利データを含むデータ記憶域）、および、特定の記憶位置にあるこの特定の権利データに対応する識別子（例えば当該の特定の権利データを含むファイルを識別する識別子）を含むことができる。この場合、権利管理コンテンツ３１０は、どこにいる誰にでも送達することができ、コンテンツを消費する権利を有するエンティティだけが、譲渡された権利に従ってのみコンテンツを消費することができる。

【００３０】

ＳＲＬ３０８はディジタル署名された文書であり、これにより改ざんできないようになっている。さらに、ＳＲＬ３０８は、コンテンツの暗号化に使用される実際の鍵タイプおよびアルゴリズムからは独立しているが、それが保護するコンテンツとの強力な１対１関係を維持する。ここで図３を参照するが、本発明の一実施形態で、ＳＲＬ３０８は、コンテンツに関する情報を含むことができる。これはＳＲＬ３０８の基礎であり、おそらくコンテンツのＩＤを含む。ＳＲＬ３０８はさらに、ＳＲＬ３０８に署名するＤＲＭサーバに関する情報を含む。これは（ＰＵ－ＤＲＭ（ＤＥＳ１））と、ネットワーク上でＤＲＭサーバを突き止めるためのＵＲＬや、ＵＲＬが失敗した場合のフォールバック情報などの参照情報とを含む。さらに、ＳＲＬ３０８はとりわけ、ＳＲＬ３０８自体を記述する情報、（ＤＥＳ１（権利データ））、（ＤＥＳ１（ＣＫ））、およびＳ（ＰＲ－ＤＲＭ）を含む。

【００３１】

信用されるエンティティが権利データに署名して署名済み権利ラベル３０８を生み出すことを確実にすることにより、ＤＲＭサーバは、権利ラベル３０８の権利データに記述されるように発行元によって示される条件に従ってコンテンツに対するライセンスを交付することを表明する。理解されるはずだが、ライセンスはコンテンツ鍵（ＣＫ）を含むので、特にユーザは、コンテンツを提供するライセンスを得る必要がある。ユーザは、暗号化済みコンテンツに対するライセンスを得たい場合、コンテンツについてのＳＲＬ３０８と、ユーザの資格を証明する証明書とを含むライセンス要求を、ＤＲＭサーバ３２０またはその他のライセンス交付エンティティに提示することができる。次いでライセンス交付エンティティは、（ＰＵ－ＤＲＭ（ＤＥＳ１））および（ＤＥＳ１（権利データ））を復号して権利データを生成し、作者（もしいれば）からライセンス要求元エンティティに供与されるすべての権利をリストし、これらの特定の権利だけを含むライセンスを構築することができる。

【００３２】

アプリケーション３０２がＳＲＬ３０８を受け取ったとき、このようなアプリケーション３０２は、署名済み権利ラベル３０８を対応する（ＣＫ（内容））３０４と連結して、権利管理されるディジタルコンテンツを形成することが好ましい。代わりに、権利データを既知の位置に記憶し、この位置への参照を暗号化済みディジタルコンテンツと共に提供してもよい。これにより、ＤＲＭ対応の提供アプリケーションが、提供しようとするコンテンツを介して署名済み権利ラベル３０８を発見することができる。この発見により、提供アプリケーションがトリガされて、ＤＲＭライセンス供与サーバ３２０に対するライセンス要求が開始する。発行アプリケーション３０２は、例えばＤＲＭライセンス供与サーバ３２０へのＵＲＬを記憶することができる。あるいは、ＤＲＭライセンス供与サーバ３２０は、権利ラベルにディジタル署名する前にそれ自体のＵＲＬをメタデータとして権利ラベルに組み込み、提供アプリケーションから呼び出されたＤＲＭクライアントＡＰＩ３０６が正しいＤＲＭサーバ３２０を識別できるようにすることもできる。権利ラベルに署名する前に、固有の識別子、例えばＧＵＩＤ（ｇｌｏｂａｌｌｙ ｕｎｉｑｕｅ ｉｄｅｎｔｉｆｉｅｒ）などを挿入することが好ましい。

【００３３】

本発明の好適な実施形態では、コンテンツ作成アプリケーション３０２または提供アプリケーションと、ＤＲＭサーバ３２０との間の通信には、ＳＯＡＰ（ｓｉｍｐｌｅ ｏｂｊｅｃｔ ａｃｃｅｓｓ ｐｒｏｔｏｃｏｌ）を使用することができる。さらに、ＤＲＭプロトコルのクライアント側を実装するのにアプリケーション３０２などのアプリケーションを必要とするのではなくローカルＡＰＩ呼出しを行うだけでよいように、ＡＰＩ３０６などのＡＰＩライブラリを設けることができる。ディジタルコンテンツについての権利記述、ライセンス、および権利ラベルを記述するためには、ＸＭＬ言語であるＸＭＬを使用することが好ましいが、権利記述およびその他のデータには、適した任意のフォーマットを使用することができることを理解されたい。

【００３４】

発行されたコンテンツに対するライセンスの取得

図４は、権利管理されるディジタルコンテンツをライセンス供与するための、本発明によるシステムおよび方法の好適実施形態の機能ブロック図である。本明細書において「ライセンス供与」という語は、ライセンス中で指名されたエンティティがライセンス中で指定された条件に従ってコンテンツを消費することを可能にするライセンスを要求し受け取るために、アプリケーションまたはサービスが従うプロセスを指す。ライセンス供与プロセスへの入力には、ライセンス要求されているコンテンツに関連する署名済み権利ラベル（ＳＲＬ）３０８と、ライセンス要求が行われているエンティティの公開鍵証明書を含めることができる。ライセンスを要求しているエンティティは、必ずしもライセンス要求が行われているエンティティであるとは限らないことに留意されたい。通常、ライセンスは、ＳＲＬ３０８からの権利記述と、暗号化済みコンテンツを復号することのできる暗号化済み鍵と、権利記述および暗号化済み鍵に対するライセンスサーバからのディジタル署名とを含む。ディジタル署名は、指定されたエンティティおよび権利が正当であることを表明する。

【００３５】

アプリケーション３０２が権利管理コンテンツ３１０を消費する方法の１つは、クライアントＡＰＩ３０６が通信ネットワーク３３０を介して権利管理コンテンツ３１０の署名済み権利ラベル３０８をＤＲＭサーバ３２０に転送するものである。ＤＲＭサーバ３２０の位置は、例えばＳＲＬ３０８中の参照情報中で知ることができる。このような実施形態では、ＤＲＭライセンス供与サーバ３２０は、後で詳述するプロセスによって、ライセンスを交付できるかどうかを権利ラベル中の権利記述を使用して決定することができ、交付できる場合は、権利記述を取り出してライセンスに含めることができる。前述のように、権利ラベル３０８は、ＤＲＭサーバ３２０の公開鍵（ＰＵ－ＤＲＭ）に従って暗号化されたコンテンツ鍵（ＣＫ）（すなわちＰＵ－ＤＲＭ（ＣＫ））を含む。ライセンスを交付するプロセスにおいて、ＤＲＭサーバ３２０は、この値を安全に復号して（ＣＫ）を得る。次いで、ライセンス要求中で渡された公開鍵証明書中の公開鍵（ＰＵ－ＥＮＴＩＴＹ）を使用して、（ＣＫ）を再暗号化する（すなわち（ＰＵ－ＥＮＴＩＴＹ（ＣＫ））。新たに暗号化されたこの（ＰＵ－ＥＮＴＩＴＹ（ＣＫ））を、サーバ３２０はライセンス中に挿入する。したがって、関連する秘密鍵（ＰＲ－ＥＮＴＩＴＹ）の保持者だけが（ＰＵ－ＥＮＴＩＴＹ（ＣＫ））から（ＣＫ）を回復することができるので、（ＣＫ）を露出する危険なしにライセンスを呼出し元に返すことができる。次いで、クライアントＡＰＩ３０６は、（ＣＫ）を使用して暗号化済みコンテンツを復号し、復号されたディジタルコンテンツ３１２を形成する。次いで、クライアントアプリケーション３０２は、ライセンス中で提供される権利に従って、復号されたディジタルコンテンツ３１２を使用することができる。

【００３６】

別法として、例えば発行クライアントなどのクライアントが、コンテンツを消費するためのそれ自体のライセンスを交付することもできる。このような実施形態では、ディジタルコンテンツを適切な状況で復号するのに必要な鍵をクライアントに提供する安全なプロセスを、クライアントコンピュータ上で実行することができる。

【００３７】
図５Ａおよび５Ｂに、権利管理されるディジタルコンテンツをライセンス供与するための、本発明による方法６００の好適な実施形態のフローチャートを提供する。本発明によれば、要求エンティティが、１つまたは複数の潜在的ライセンス取得側に代わってライセンス要求をサブミットすることができる。要求エンティティは、潜在的ライセンス取得側の１つであっても、そうでなくてもよい。潜在的ライセンス取得側は、個人、グループ、デバイス、または、任意のスキームでコンテンツを消費することのできる任意のこのようなエンティティとすることができる。ここで、ＤＲＭサーバがライセンス要求を処理する一実施形態に関して方法６００を説明するが、ライセンス要求の処理をクライアント上で実施し、クライアントがライセンスを交付することもできることを理解されたい。

【００３８】
ステップ６０２で、例えばＤＲＭサーバなどのライセンス交付エンティティが、ライセンス要求を受け取る。ライセンス要求は、要求が行われている１つまたは複数のライセンス取得側それぞれについての公開鍵証明書と識別のどちらかを含むことが好ましい。

【００３９】
ステップ６０４で、要求エンティティ（すなわちライセンス要求を行っているエンティティ）を認証する。本発明の一実施形態によれば、ライセンス交付エンティティは、プロトコル（例えばチャレンジ－レスポンス）認証を用いて要求エンティティの識別を決定するように構成することもでき、あるいは、要求エンティティの認証を必要としないように構成することもできる（「匿名認証を可能にする」とも言われる）。認証を必要とする場合は、任意のタイプの認証スキームを使用することができる（例えば前述のチャレンジ－レスポンススキームや、ＭＩＣＲＯＳＯＦＴ．ＮＥＴ、ＰＡＳＳＰＯＲＴ、ＷＩＮＤＯＷＳ（登録商標）認証×５０９などのユーザＩＤおよびパスワードスキーム）。匿名認証を可能にし、および、統合情報システムによってサポートされる任意のプロトコル認証スキームをサポートすることが好ましい。認証ステップの結果は、例えば「匿名」識別（匿名認証の場合）や個人アカウント識別などの識別となる。何らかの理由でライセンス要求を認証することができない場合は、エラーを返し、ライセンスは供与しない。

【００４０】
ステップ６０６で、認証された識別を許可する。すなわち、ステップ６０４で認証された識別が（それ自体でまたは別のエンティティの代わりに）ライセンスを要求することができるかどうかを決定する。ライセンス交付エンティティは、ライセンスを要求することが許可される（または許可されない）エンティティのリストを記憶していることが好ましい。好適な実施形態では、この識別リスト中の識別は、ライセンス要求が行われている１つのエンティティの識別ではなく、要求を行っている１つのエンティティの識別であることが好ましいが、このどちらでもよい。例えば、個人アカウント識別が直接にライセンス要求を行うことは許可されないが、信用されるサーバプロセスがこのようなエンティティに代わってライセンス要求を行うことはできるものとすることができる。

【００４１】
本発明によれば、ライセンス要求は、潜在的ライセンス取得側それぞれについての公開鍵証明書と識別のどちらかを含むことができる。１つのライセンス取得側だけのためにライセンスが要求される場合は、１つの証明書または識別だけが指定される。複数のライセンス取得側のためにライセンスが要求される場合は、それぞれの潜在的ライセンス取得側について証明書または識別を指定することができる。

【００４２】
ライセンス交付エンティティは、有効な各ライセンス取得側についての公開鍵証明書を有することが好ましい。しかし、アプリケーション３０２は、所与のユーザのためのライセンスを生成したいと思ってもこのユーザについての公開鍵証明書にアクセスできない場合がある。このような状況では、アプリケーション３０２は、このユーザの識別をライセンス要求中で指定することができる。この結果、ライセンス交付エンティティは登録済み証明書プラグインモジュールを呼び出すことができ、このプラグインモジュールは、ディレ

クトリサービスを検索して適切なユーザの公開鍵証明書を返す。

【００４３】

ステップ６０８で、ライセンス要求に公開鍵証明書が含まれていないとライセンス交付エンティティが決定した場合、交付エンティティは、指定された識別を使用して、ディレクトリサービスまたはデータベース中で適切な公開鍵証明書を検索する。ステップ６１０で、証明書がディレクトリ中にあると交付エンティティが決定した場合は、ステップ６１２でこの証明書を取り出す。好適な実施形態では、証明書プラグインを使用して、ディレクトリアクセスプロトコルによって公開鍵証明書をディレクトリサービスから取り出す。所与の潜在的ライセンス取得側についての証明書が要求中にもディレクトリ中にも見つからない場合は、ライセンスサーバはこの潜在的ライセンス取得側に対してライセンスを生成せず、ステップ６１４で要求エンティティにエラーを返す。

【００４４】

ライセンス交付エンティティが少なくとも１つの潜在的ライセンス取得側についての公開鍵証明書を有すると仮定すると、ステップ６１６で、交付エンティティはこのライセンス取得側の信用を妥当性検査する。好ましくは、交付エンティティは、信用される証明書交付者の証明書のセットを有するように構成され、信用される交付者のリスト中にライセンス取得側の証明書の交付者があるかどうかを決定する。ステップ６１６で、信用される交付者のリスト中にライセンス取得側の証明書の交付者がないと交付エンティティが決定した場合は、このライセンス取得側についての要求は失敗し、ステップ６１４でエラーが生成される。したがって、信用される交付者によってその証明書が交付されていない潜在的ライセンス取得側は、ライセンスを受け取らないことになる。

【００４５】

さらに、交付エンティティは、信用される交付者の証明書から個々のライセンス取得側の公開鍵証明書までの証明書チェイン中のすべてのエンティティに対してディジタル署名の妥当性検査を行うことが好ましい。チェイン中でディジタル署名を妥当性検査するプロセスは、周知のアルゴリズムである。所与の潜在的ライセンス取得側についての公開鍵証明書の妥当性が認められない場合、またはチェイン中の証明書の妥当性が認められない場合は、この潜在的ライセンス取得側は信用されず、したがってこの潜在的ライセンス取得側にライセンスは交付されない。そうでない場合は、ステップ６１８でライセンスを交付することができる。このプロセスは、ステップ６２０で、ライセンス要求が行われているすべてのエンティティが処理されるまで繰り返す。

【００４６】

図５Ｂに示すように、ライセンス交付エンティティは、ライセンス要求中で受け取った署名済み権利ラベル３０８の妥当性検査に進む。好適実施形態では、交付エンティティは、権利ラベルプラグインおよびバックエンドデータベースを使用して、交付エンティティが署名したあらゆる権利ラベルのマスタコピーをサーバ上に記憶することができる。権利ラベルは、発行時に挿入されたＧＵＩＤで識別される。ライセンス時（ステップ６２２）、交付エンティティは、ライセンス要求中の権利ラベル入力を解析し、そのＧＵＩＤを取り出す。次いでこのＧＵＩＤを権利ラベルプラグインに渡し、権利ラベルプラグインは、データベースに対する照会を発行して、マスタ権利ラベルのコピーを取り出す。マスタ権利ラベルは、ライセンス要求中で送られた権利ラベルのコピーよりも最新のものとすることができ、これが以下のステップにおいて要求中で使用される権利ラベルになる。権利ラベルがデータベース中でＧＵＩＤに基づいて見つからない場合は、ステップ６２４で、交付エンティティはそのポリシーをチェックして、要求中の権利ラベルに基づいてライセンスを交付することがまだ許可されるかどうかを決定する。ポリシーがこれを許可しない場合は、ステップ６２６でライセンス要求は失敗し、ステップ６２８でエラーがＡＰＩ３０６に返される。

【００４７】

ステップ６３０で、ライセンス交付エンティティは権利ラベル３０８を妥当性検査する。権利ラベル上のディジタル署名を妥当性検査し、ライセンス交付エンティティが権利ラベ

ルの交付者（それに署名したエンティティ）でない場合は、ライセンス交付エンティティは、権利ラベルの交付者が別の信用されるエンティティ（例えばライセンス交付エンティティが鍵材料を共有できるようになっているエンティティ）かどうかを決定する。権利ラベルの妥当性が認められない場合、または信用できるエンティティによって交付されたものでない場合は、ステップ６２６でライセンス要求は失敗し、ステップ６２８でエラーがＡＰＩ３０６に返される。

【００４８】

すべての妥当性検査を行った後、ライセンス交付エンティティは、権利ラベル３０８を、承認された各ライセンス取得側に対するライセンスに変換する。ステップ６３２で、ライセンス交付エンティティは、各ライセンス取得側に交付するライセンスについて各権利記述を生成する。各ライセンス取得側につき、交付エンティティは、そのライセンス取得側の公開鍵証明書中で指定された識別を、権利ラベル中の権利記述中で指定された識別に対して評価する。権利記述は、あらゆる権利または権利セットに、ライセンス中の、その権利または権利セットを実施することのできる識別のセットを割り当てる。このライセンス取得側の識別が関連するあらゆる権利または権利セットにつき、その権利または権利セットが、このライセンスについての新しいデータ構造中にコピーされる。得られるデータ構造が、この特定のライセンス取得側に対するライセンス中の権利記述である。このプロセスの一部として、ライセンス交付エンティティは、権利ラベルの権利記述中のいずれかの権利または権利セットと関連するかもしれない前提条件があればそれを評価する。例えば、ある権利には、ライセンス交付エンティティが指定時間以後にライセンスを交付することを制限する時間前提条件が関連するものとすることができる。この場合、交付エンティティは現在時間をチェックする必要があり、前提条件に指定された時間を過ぎていれば、交付エンティティは、ライセンス取得側の識別がその権利に関連していても、このライセンス取得側に権利を交付することはできない。

【００４９】

ステップ６３６で、交付エンティティは、（ＰＵ－ＤＲＭ（ＤＥＳ１））および（ＤＥＳ１（ＣＫ））を権利ラベル３０８からとり、（ＰＲ－ＤＲＭ）を適用して（ＣＫ）を得る。次いで交付エンティティは、（ＰＵ－ＥＮＴＩＴＹ）すなわちライセンス取得側の公開鍵証明書を使用して（ＣＫ）を再暗号化し、その結果（ＰＵ－ＥＮＴＩＴＹ（ＣＫ））を得る。ステップ６３８で、交付エンティティは、生成した権利記述を（ＰＵ－ＥＮＴＩＴＹ（ＣＫ））と連結し、得られたデータ構造に（ＰＲ－ＤＲＭ）を使用してディジタル署名する。この署名済みデータ構造が、この特定のライセンス取得側エンティティに対するライセンスである。

【００５０】

ステップ６４０で、特定の要求について生成するライセンスがそれ以上ないと交付エンティティが決定したとき、交付エンティティは０個またはそれ以上のライセンスを生成したことになる。ステップ６４２で、生成したライセンスを、これらのライセンスに関連する証明書チェイン（例えば、サーバ自体の公開鍵証明書、ならびにその証明書を交付した証明書など）と共に要求エンティティに返す。

【００５１】

本発明によるシステムの好適な実施形態では、ライセンス供与側の鍵を複数使用することができる。このような実施形態では、暗号化されて権利ラベル３０８を通りライセンス中に入るコンテンツ鍵（ＣＫ）は、実際、任意のどんなデータとすることもできる。特に有用な一変形は、暗号化された別個のコンテンツ鍵（ＣＫ）を複数使用するものであり、コンテンツ鍵（ＣＫ）はそれぞれ、権利記述中の異なる権利または異なる当人に関連する。例えば、アルバムの歌のディジタルバージョンをすべて異なる鍵（ＣＫ）で暗号化することができる。これらの鍵（ＣＫ）は、同じ権利ラベル中に含まれることになるが、ある当人は、これらの歌のうちの１つを再生する権利を有することができ（例えば、彼は自分のライセンス中で１つの鍵を得る権利しか有さない）、第２の当人は、すべての歌を再生する権利を有する（彼女は自分のライセンス中ですべての鍵を得る権利を有する）。

【００５２】
本発明によるシステムでは、発行アプリケーション／ユーザが、ライセンス取得側のグループまたは種類を権利ラベル３０８中で指定できることが好ましい。このような実施形態では、ライセンス交付エンティティは、権利ラベル中で指定されたどんなグループ／種類も評価して、現在のライセンス取得側の識別がこれらのグループまたは種類のメンバであるかどうかを決定する。指定されたグループ／種類中のメンバシップが見つかった場合は、交付エンティティは、このグループ／種類に関連する権利または権利セットを、ライセンスに使用される権利記述データ構造に加えることができる。
【００５３】
本発明の好適な実施形態では、ＤＲＭサーバ中の発行プロトコルインタフェースおよびライセンスプロトコルインタフェースが、呼出し側アプリケーションまたはユーザの認証および許可をサポートし、ＤＲＭサーバのための管理コンソールにより、管理者は、ライセンス供与インタフェースと発行インタフェースの両方についてのアクセス制御リストを生成することができる。これにより、サーバの顧客は、どのユーザ／アプリケーションが発行またはライセンス供与、あるいはその両方を行うことができるかに関するポリシーを適用することができる。
【００５４】
例示的なプラットフォーム、ならびにこれと識別およびライセンスとの関係
本発明がサポートする信用モデルは、権利管理されるコンテンツの保護が、コンテンツを保護する鍵の保護に依存するという考えに基づく。先に論じたように、コンテンツは、ユーザの提供する対称鍵ＣＫで暗号化される。コンテンツの最終的な消費者はコンテンツを復号するためにＣＫを必要とするので、ＤＲＭシステムが解決しなければならない問題の１つは、鍵が移送中に見られないように、およびコンテンツ消費者が鍵を悪用しないように、どのようにして鍵を安全なスキームで消費者に提供するかである。図６～８に、鍵ＣＫを安全なスキームでユーザに提供するために使用することのできる構造を示す。
【００５５】
図６には、暗号サービスを提供する例示的なプラットフォーム６０２を示す。プラットフォーム６０２は、公開／秘密鍵の対であるＰＵ－ＰＬＡＴＦＯＲＭ／ＰＲ－ＰＬＡＴＦＯＲＭと、この鍵の対を適用して暗号サービスを実施する暗号モジュール６０４を含む。プラットフォーム６０２の機能は、秘密のプラットフォーム鍵ＰＲ－ＰＬＡＴＦＯＲＭを明かさずにこれらの暗号サービスを実施することである。したがって、プラットフォーム６０２を利用するオブジェクトは、暗号要求（例えばコンテンツを復号する要求や、ディジタル署名を検証する要求）を提供し、暗号結果（例えば復号されたコンテンツや署名検証）を受け取る。プラットフォーム６０２は、秘密のプラットフォーム鍵ＰＲ－ＰＬＡＴＦＯＲＭをユーザに明かさずに結果を提供するので、「ブラックボックス」と呼ばれることもある。
【００５６】
プラットフォーム６０２は様々な実装形態を有することができ、本発明によりこれらの実装形態のいずれを使用することもできる。例えばプラットフォーム６０２は、改ざん防止が施されたソフトウェアのようなものとすることができ、秘密プラットフォーム鍵を隠された形で含み、コード難読化技法を用いて、ハッカーがソフトウェアを分析することによって秘密鍵を知ろうとするのを困難にする。別の例として、プラットフォーム６０２は自己完結型の集積回路とすることができ、分析を受けないよう回路を保護する、および／または防壁侵入が試みられた場合に回路を自己破壊させる、物理防壁が付いたものとすることができる。権利管理されるコンテンツがコンピュータ上で使用可能な場合に、各コンピュータは、固有の鍵の対を備えたこのようなプラットフォームを１つ有することが期待される。秘密鍵を保護するのに使用される手段にかかわらず、前述の暗号機能を実施する任意のプラットフォームを本発明により使用することができる。ただし、図９に関連して後述するが、秘密鍵の保護に使用される手段はプラットフォームの信用に影響する。
【００５７】

図７に、例示的な識別証明書７０２を示す。識別証明書７０２は、ペルソナについての識別を定義する。この場合、人物はｊｏｈｎ@ｍｉｃｒｏＳｏｆｔ．ｃｏｍであり、したがって、ｊｏｈｎ@ｍｉｃｒｏＳｏｆｔ．ｃｏｍが権利管理コンテンツに対するライセンスを得たいときは、識別証明書７０２が、このライセンスを作成することになるＤＲＭサーバに対してｊｏｈｎ@ｍｉｃｒｏＳｏｆｔ．ｃｏｍが自分を識別するのに使用するデータ構造である。識別証明書７０２は、公開鍵ＰＵ－ＥＮＴＩＴＹについての公開鍵証明書と、プラットフォームの公開鍵ＰＵ－ＰＬＡＴＦＯＲＭで暗号化された秘密鍵ＰＲ－ＥＮＴＩＴＹと、識別証明書７０２の交付者のディジタル署名（この交付者の秘密鍵ＰＲ－ＩＳＳＵＥＲを使用して生み出される）とを含む。

【００５８】

図４、５Ａ、５Ｂに関連して先に論じたように、ライセンス要求中、ＰＵ－ＥＮＴＩＴＹを含む証明書がＤＲＭサーバに渡される。識別証明書７０２は、このような証明書の例である。したがってＰＵ－ＥＮＴＩＴＹは、ステップ６３６（図５Ｂに示す）でコンテンツ鍵ＣＫを暗号化するのに使用される鍵である。識別証明書７０２はユーザのマシンにインストールされることになるので、ユーザがＰＲ－ＥＮＴＩＴＹへの直接アクセスを有さないことが重要である。というのは、ＰＲ－ＥＮＴＩＴＹを有する者は誰でもライセンス中のコンテンツ鍵ＣＫを復号してコンテンツの保護を損なうことができるからである。このため、プラットフォーム６０２がライセンスからＣＫを復号するためにＰＲ－ＥＮＴＩＴＹが必要になったときにＰＲ－ＥＮＴＩＴＹを復号することができるように、識別証明書７０２は、ＰＵ－ＰＬＡＴＦＯＲＭで暗号化されたＰＲ－ＥＮＴＩＴＹを記憶している。ＰＲ－ＥＮＴＩＴＹを有する者は誰でもコンテンツを盗む力を持つので、識別証明書７０２中のディジタル署名は、ＰＲ－ＥＮＴＩＴＹが保護されており、安全でないプラットフォームに配布されていないという、証明書交付者の保証を表す。

【００５９】

識別証明書７０２は、ユーザのコンピュータをユーザの識別から分離することをサポートすることに留意されたい。したがって、ｊｏｈｎ@ｍｉｃｒｏＳｏｆｔ．ｃｏｍは、複数のプラットフォーム用に証明書が再作成されるようにするだけで、自分の識別が複数のコンピュータにインストールされるようにすることができる（同じ識別に対して交付できる証明書の数、またはこのような証明書をインストールできるプラットフォームのタイプを制限する識別プラットフォームがある場合もある）。これらの様々な証明書は、証明書中のＰＲ－ＥＮＴＩＴＹを暗号化する公開鍵ＰＵ－ＰＬＡＴＦＯＲＭがプラットフォームごとに異なることを除いては同じとなる。さらに、識別証明書７０２はグループ識別を生み出すこともサポートする。例えば、自動車会社の自動車部品部門が識別を有することができる。これにより、自動車部品部門にいる全員のコンピュータに自動車部品識別証明書がインストールされるようにするだけで、自動車部品部門の全体に文書をライセンス供与することができ、および消費可能にすることができる。

【００６０】

図８に、識別に交付されるライセンス８０２を示す。ライセンス８０２は、権利（すなわち、コンテンツで何ができるか、およびコンテンツを消費することのできる状況を律する規則）と、ＰＵ－ＥＮＴＩＴＹによって暗号化されたコンテンツ鍵ＣＫと、ライセンスを交付したＤＲＭサーバの秘密鍵ＰＲ－ＤＲＭを使用して生み出された署名を含む。図８でわかるように、ＣＫは、秘密の識別鍵ＰＲ－ＥＮＴＩＴＹを使用してＰＵ－ＥＮＴＩＴＹ（ＣＫ）を復号することによってのみ、ライセンスから回復することができる。したがって、これがライセンスからＣＫを回復する唯一の方法なので、実際、ライセンスを使用するにはＰＲ－ＥＮＴＩＴＹを含む識別証明書７０２がなければならない。さらに、識別証明書７０２中のＰＲ－ＥＮＴＩＴＹは公開プラットフォーム鍵ＰＵ－ＰＬＡＴＦＯＲＭで暗号化されるので、識別証明書は、コンテンツが消費されるプラットフォーム６０２用に限定して生み出されなければならない。このため、ライセンスを使用してコンテンツを消費するには、ユーザには、自分の識別に交付されたライセンスと、コンテンツが消費されるプラットフォームに交付された識別証明書がなければならない。

【００６１】
信用のモデル
前述のＤＲＭシステムは、複数の鍵の層を介してコンテンツを保護する。これらの鍵の層は、コンテンツ所有者からコンテンツが最終的に使用されるプラットフォームに至る信用関係のチェインを表す。図９に、様々な鍵の間の関係と、これらの鍵が意味する信用のチェインを示す。
【００６２】
図９に示すように、コンテンツ９０２は、コンテンツ鍵９０４（前の考察でＣＫと呼んでいた）で保護される。コンテンツ鍵９０４は、識別鍵の対９０６（ＰＵ－ＥＮＴＩＴＹ／ＰＲ－ＥＮＴＩＴＹ）で保護される。秘密の識別鍵は、プラットフォーム鍵の対９０８（ＰＵ－ＰＬＡＴＦＯＲＭ、ＰＲ－ＰＬＡＴＦＯＲＭ）で保護される。先に論じたように、秘密の識別鍵（ＰＲ－ＥＮＴＩＴＹ）は、コンピューティングデバイス上で識別証明書内に記憶されて、コンピューティングデバイスの公開プラットフォーム鍵で、すなわちＰＵ－ＰＬＡＴＦＯＲＭ（ＰＲ－ＥＮＴＩＴＹ）として暗号化されることが好ましい。これにより、ＰＲ－ＥＮＴＩＴＹはＰＲ－ＰＬＡＴＦＯＲＭでしか復号することができない。
【００６３】
コンテンツ９０２からプラットフォーム鍵の対９０８までの保護チェインにおけるどんな脆弱性も、コンテンツ９０２のセキュリティを脅かすことは容易に理解されるであろう。したがって、コンテンツ鍵９０４が公に知られた場合、誰でもコンテンツ９０２を復号することができる。同様に、秘密の識別鍵が公に知られた場合、誰でもコンテンツ鍵９０４を復号することができ、次にコンテンツ９０２を復号することができる。最後に、秘密のプラットフォーム鍵が公に知られた場合、誰でも秘密の識別鍵を復号することができ、それによりコンテンツ鍵を復号することができ、それによりコンテンツを復号することができる。このため、これらの暗号化の層を介してコンテンツへのアクセスを与えることについてのセキュリティは、コンテンツ鍵、秘密の識別鍵、および秘密のプラットフォーム鍵が損なわれないことに依存する。
【００６４】
したがって、保護すべきこれらの各鍵の機能は、信用のチェインを介して確立される。このチェインを図９の要素９１２から９１８に示す。コンテンツ所有者９１２は、コンテンツを発行するときにコンテンツ鍵ＣＫを生み出し、この鍵を、署名のために権利ラベルが提示されるときにライセンス供与側（すなわちＤＲＭサーバ）と共有する。したがって、コンテンツ所有側９１２は、コンテンツへの自由なアクセスを与えたくないので、ライセンス供与側９１４がコンテンツ鍵を損なわないものと実質的に信用する。すなわち、制御された状況下でのみコンテンツ鍵を配布するものと信用する。同様に、ライセンス供与側は、特定の識別にライセンスを交付するとき（必然的に、秘密の識別鍵を使用してコンテンツ鍵を復号できるような形でコンテンツ鍵を分与することを含む）、秘密の識別鍵が適切な制御条件下でのみ使用できるように、識別証明書の交付者９１６が識別証明書を交付したことを本質的に信用する。証明書交付者９１６は、所与のプラットフォーム９１８に識別証明書を交付するとき（それによりプラットフォームが秘密の識別鍵ＰＲ－ＥＮＴＩＴＹを使用できるようにするとき）、プラットフォーム９１８が秘密鍵を悪用しないことを信用する。
【００６５】
コンテンツを悪用から完璧に守る権利管理システムはない。どんな権利管理システムも、十分な時間、スキル、リソース、および動機を有する敵によって破られる可能性がある。しかし、権利管理システムの性質上、コンテンツ所有者９１２は、処理チェインに関係する様々なエンティティ（例えばこの例ではランセンス供与側９１４、識別証明書交付者９１６、およびプラットフォーム９１８）が、これらのエンティティに信用をおけるほど十分にうまく完全にそれぞれの鍵を保護するかどうかを決定することができる。したがってコンテンツのセキュリティは、どのエンティティを信用し、どのエンティティを信用しないかに直接に依存することが容易に理解できる。

【００６６】
後述するように、本発明は、特定の信用関係のタイプを確立（または拒否）することに基づいてコンテンツを交付するためのシステムおよび方法を提供する。
【００６７】
複数の識別サーバ間における信用の考慮
先に論じたように、誰を信用し誰を信用しないかを決定することによって部分的に、セキュリティスキームを定義することができる。これらの信用決定の一面は、識別証明書の特定の交付者によって交付されるこのような証明書を信用するかどうかを、ライセンス供与側が決定することである。この信用決定は重要である。というのも、ライセンス供与側は識別証明書の公開鍵（ＰＵ－ＥＮＴＩＴＹ）でコンテンツを暗号化することになり、したがって、対応する秘密鍵（ＰＲ－ＥＮＴＩＴＹ）が不正な人の手に落ちないようにする手段が講じられない限り、全世界が暗号化済みコンテンツにアクセスできることになるからである。
【００６８】
図１０に、識別証明書１および２（参照番号１００４（１）および１００４（２））を交付する複数の識別サーバ１００２（１）および１００２（２）を示す。この例では、識別証明書１はエンティティ「ジョー」に向けたものであり、識別証明書２はエンティティ「フレッド」に向けたものである。このような識別は「ペルソナ」と呼ぶこともできる。図示の例示的なペルソナは個人だが、前の考察から、識別証明書は「グループエンティティ」または「グループペルソナ」（「自動車部品部門」など）を定義することもできることは理解されるであろう。各識別証明書は、（相対的に）固有である鍵の対に関連し、識別証明書自体がこの鍵の対の公開部分を含む。したがって、識別証明書１は公開鍵ＰＵ－ＪＯＥを含み、識別証明書２は公開鍵ＰＵ－ＦＲＥＤを含む。（図７に関連して先に論じたように、識別証明書は鍵の対の秘密部分を含むこともできる。ただしユーザは秘密鍵への自由なアクセスを有するべきではないので、平文で含まないことが好ましい。）さらに、各識別証明書は署名を含む。署名は、（少なくとも）この公開鍵に対して取り入れられる。各証明書は、その交付者の署名を含む。したがって、識別証明書１は識別サーバ１の秘密鍵（ＰＲ－ＩＳ１）で署名されており、識別証明書２は識別サーバ２の秘密鍵（ＰＲ－ＩＳ２）で署名されている。識別サーバ１および２がこれらの識別証明書に署名するとき、これらは本質的に、これらの識別証明書についての秘密鍵が損なわれないよう保護することを表明している。
【００６９】
識別サーバによっては、生み出したエンティティ用の秘密鍵のセキュリティを確保することにおいてより優れている（またはより劣る）場合がある。図１０の例では、識別サーバ１は「強いセキュリティプロシージャ」を有し、識別サーバ２は「緩いセキュリティプロシージャ」を有する。これらのプロシージャの相対的な強度（または緩さ）は、どんな形を取る可能性もある。例えばおそらく、識別サーバ１は、物理的に安全なプラットフォーム鍵を有することがわかっているデバイスだけに秘密鍵をインストールし、識別サーバ２は、秘密鍵の取得側の信用を検証せずに、および／または秘密鍵がインストールされることになるプラットフォームのタイプを検証せずに、平文で秘密鍵を渡す場合がある。これらは、異なる識別サーバのセキュリティプロシージャの相対的な有効性がどれほど違うかということの一例である。
【００７０】
識別サーバ間のセキュリティにおけるこれらの違いにより、ＤＲＭサーバは、いくつかの識別サーバは信用でき、いくつかは信用できないと決定することができる。それによりＤＲＭサーバは、信用する識別サーバによって署名された識別証明書だけにライセンスを交付することができる。図１０の例では、識別サーバ１は強いセキュリティプロシージャを有するが、識別サーバ２は緩いセキュリティプロシージャを有するので、ＤＲＭサーバ３２０は、識別サーバ１は信用するが識別サーバ２は信用しない。このためＤＲＭサーバ３２０は、識別サーバ１の秘密鍵で署名された識別証明書だけに対するライセンスを交付す

る。

【００７１】

図１０では、サーバ１とサーバ２がそれぞれ「強い」「緩い」セキュリティプロシージャを有するものとして示してあるが、識別サーバの選択的な信用は「緩い」対「強い」に基づく必要はないことに留意されたい。例えば、サーバ１とサーバ２は、一方のサーバのセキュリティ機能が他方よりも明確に「強い」とは言えないとしても、単にセキュリティや認証などに関して異なる機能を有するだけでもよい。それでもやはりＤＲＭサーバ３２０は、どの識別サーバを信用しどの識別サーバを信用しないかに関して選択をする資格を有する。例えば、２つのシステムが、両方とも強いセキュリティプロシージャを有するが、異なるようにユーザを認証する場合がある。例えば一方のシステムはスマートカードを必要とし、他方のシステムはＸ５０９証明書を必要とする。この違いは、ＤＲＭサーバ３２０を運営するエンティティにとって重要であることがある。したがって、識別サーバを信用するためにそのセキュリティの強度に基づいて選択することが本発明の典型的な使用法であることは理解されたいが、これは、ＤＲＭサーバ３２０が信用するためにいくつかの識別サーバを選択して他の識別サーバを選択しないことの多くの理由の１つに過ぎない。

【００７２】

図１１に、どの識別サーバを信用できるかについての決定が、２つの組織によって文書を共有できる方法に影響を及ぼす例を示す。２つの会社「会社Ａ」および「会社Ｂ」は、その従業員が文書を共有できるようにしたいと思っており、これらの文書へのアクセスは、ＤＲＭシステムによって制御される。会社Ａの従業員は、会社Ａの識別サーバ１１０２によって交付される識別を有し、会社Ｂの従業員は、会社Ｂの識別サーバ１１０４によって交付される識別を有する。さらに、各会社は、ＤＲＭ制御される文書を閲覧するためのライセンスを交付するそれ自体のＤＲＭサーバを有する。通常、会社ＡのＤＲＭサーバ１１０６は、会社Ａの識別サーバ１１０２を信用するようにセットアップされ、会社ＢのＤＲＭサーバ１１０４は、会社Ｂの識別サーバ１１０８を信用するようにセットアップされる。

【００７３】

典型的なシナリオでは、会社Ａの従業員が、１つのコンテンツに対するライセンスを得るために、会社ＡのＤＲＭサーバ１１０６に署名済み権利ラベルを提示する。この従業員は、会社Ａの識別サーバ１１０２によって交付された識別（すなわち、鍵の対ＰＵ－ＥＮＴＩＴＹ／ＰＲ－ＥＮＩＴＩＴＹを含む識別証明書）を有する。署名済み権利ラベルによってこの従業員へのライセンス交付が許可されると仮定すると、会社ＡのＤＲＭサーバ１１０６は、会社Ａの識別サーバ１１０２を信用するので、この従業員の識別証明書のためのライセンスを作成することができる。しかし、会社Ａのある従業員がコンテンツを発行し、この文書の使用許可を会社Ｂの従業員に与えたいとする。会社Ａの従業員がこのコンテンツについての権利ラベルを生み出すとき、この権利ラベルは、コンテンツの許可ライセンス取得側の１人として会社Ｂの従業員のペルソナを指定することができる。しかし、会社Ｂの従業員は会社Ｂの識別サーバ１１０４によって交付された識別証明書を有し、会社ＡのＤＲＭサーバ１１０６は会社Ｂの識別サーバ１１０４を（まだ）信用しないので、会社Ｂのこの従業員がライセンスを得るために会社ＡのＤＲＭサーバ１１０６に接触しても、会社ＡのＤＲＭサーバ１１０６は、この従業員の識別証明書に対してライセンスを交付することができない。（図１３～１４に関連して後で論じるように、会社ＢのＤＲＭサーバが会社Ａで発行されたコンテンツに対するライセンスを交付できるようにすることも可能だが、そうするには会社Ａと会社Ｂがそれらの秘密鍵を共有する必要があり、これは状況によっては望ましくない。）

【００７４】

解決法は、会社ＡのＤＲＭサーバ１１０６と会社Ｂの識別サーバ１１０４との間に信用関係を確立することである。会社Ａは、会社Ｂの識別サーバ１１０４が識別交付時に適切なセキュリティ手段をとると確信するステップを実施することが好ましい。会社Ｂの識別サーバが会社Ａのセキュリティ基準を満たすことを会社Ａが確信すると仮定すると、会社Ａ

のＤＲＭサーバ１１０６は、会社Ｂの識別サーバ１１０４を信用することができる。この信用関係により、会社Ａの従業員は、会社Ｂの従業員にライセンス供与できる文書を発行することができる。同様に、会社ＢのＤＲＭサーバ１１０８は、会社Ａの識別サーバ１１０２を信用することができ、それにより会社Ｂの従業員は、会社Ａにライセンス供与できる文書を発行することができる。

【００７５】

信用関係は、各ＤＲＭサーバが、信用される識別サーバのリスト１１１０および１１１２を維持するようにすることによって確立することができる。各識別サーバは、鍵の対を有し、その鍵の対の公開部分によって識別することができる。会社Ａの識別サーバは鍵の対ＰＵ－Ａ／ＰＲ－Ａを有し、会社Ｂの識別サーバは鍵の対ＰＵ－Ｂ／ＰＲ－Ｂを有する。各識別証明書は、その証明書を交付した識別サーバの公開鍵証明書を含むことが好ましい。これにより所与の識別証明書について、ＤＲＭサーバは、その識別証明書中で示される識別サーバ公開鍵を、信用される識別サーバのリスト上にある公開鍵と比較することにより、その識別証明書を交付した識別サーバを信用するかどうかを決定することができる。（識別サーバは、交付した識別証明書に含める別個の識別子を有することもできる。ＤＲＭサーバは、公開鍵、識別子、またはその両方に基づいて、どの識別サーバが識別証明書を交付したかを決定することができる。）信用される識別サーバのリストは、「信用ペルソナ領域」と呼ぶことができる。

【００７６】

したがって、会社Ａは、会社Ｂの識別サーバを会社Ａの信用リストに載せることにより、その従業員が会社Ｂの従業員に向けてコンテンツを発行できるようにすることができる（会社Ｂの従業員が会社Ｂの識別サーバによって交付された識別証明書を有すると仮定した場合）。同様に、会社Ｂは、会社Ａの識別サーバをその信用リストに加えることができる。したがって図１１には、公開鍵ＰＵ－Ｂが会社Ａの信用リスト１１１０に加えられ、公開鍵ＰＵ－Ａが会社Ｂの信用リスト１１１２に加えられていることが示してある。

【００７７】

通常なら信用される識別サーバによって交付された特定の証明書の除外

先に論じたように、ＤＲＭサーバは、いくつかの識別サーバを選択的に信用したり／信用しなかったりする。この選択的な信用／不信モデルの注目すべき改良は、特定の識別サーバに与えられる一般的な信用から特定の識別を除外することに関するものである。例えばＤＲＭサーバは、特定の識別サーバを一般に信用するが、特定のｅメールアドレスやドメインなどに登録されたある種の証明書にはライセンスを交付したくない場合がある。唯一の例ではないがこの一例には、ｅメールアドレスに基づいて公衆に識別を交付する識別サーバの場合がある。ＭＩＣＲＯＳＯＦＴ．ＮＥＴ ＰＡＳＳＰＯＲＴは、このような識別サーバの例である。

【００７８】

図１２に、識別サーバ１２０２および１２０４を示す。識別サーバ１２０２は、例えば、ユーザから提供されたｅメールアドレスおよびパスワードに基づいて識別証明書を交付する、ｅメールアドレスに基づく公用の識別サーバとすることができる。例えば、ユーザは、ｅメールアドレス（例えばＸＸＸ@ｈｏｔｍａｉｌ．ｃｏｍ）およびパスワードを事前登録している。識別サーバ１２０２は、単にｅメールアドレスおよびパスワードを入力するようユーザに促すだけでよく、ユーザが正しいｅメールアドレス／パスワードの組合せを入力した場合は、それ以上の厳格なユーザ認証を要求することなく識別証明書を交付することができる。ｅメールアドレスに基づく公用の識別サーバ１２０２はまた、プラットフォームのセキュリティ機能を考慮せずに、ユーザの要求するどんなプラットフォームにも識別証明書をインストールすることができる場合があるという、セキュリティ上の欠点を有することがある。この技法は、識別証明書を交付する方法として相対的に安全でない方法であると考えられる。

【００７９】

対照的に、識別サーバ１２０４は高セキュリティ識別サーバである。識別サーバ１２０４

は、識別証明書を交付する前に、相対的に厳格なチェックを必要とする。例えば、ユーザは自分（および自分のコンピュータ）を（人間の）システム管理者に個人的に提示しなければならず、システム管理者は、そのコンピュータが十分に安全でありユーザがこのような識別を与えられる資格を有すると確信した場合に、サーバ１２０４によって識別証明書がユーザのコンピュータにインストールされるようにする。ユーザは、指紋やスマートカードなどを使用して自分を証明しなければならないこともある。あるいは、サーバ１２０４が会社のための識別サーバである場合、ユーザは、インターネットではなく社内イントラネットを介してサーバ１２０４にアクセスしなければならない。したがって、高セキュリティサーバ１２０４は、ｅメールアドレスに基づくサーバ１２０２よりも相対的により安全であることがわかる。

【００８０】

図１２の例では、プラットフォーム１（参照番号１２０６）は、ｅメールに基づく識別サーバから識別証明書を入手し、プラットフォーム２（参照番号１２０８）は、高セキュリティの識別サーバから識別証明書を入手する。先に論じたように、各識別証明書はその交付者の公開鍵証明書を組み込んでおり、交付者の秘密鍵で署名されているので、これらの証明書の交付者は、証明書自体から決定することができる。（図１２の例では、ｅメールアドレスに基づく公用サーバ１２０２は鍵の対ＰＵ－ＩＳ１／ＰＲ－ＩＳ１を有し、高セキュリティの識別サーバ１２０４は鍵の対ＰＵ－ＩＳ２／ＰＲ－ＩＳ２を有する。）したがって、プラットフォーム１および２がライセンス要求１２１０（それぞれの識別証明書を含む）をＤＲＭサーバ３２０に送ることによって何らかのコンテンツに対するライセンスを得ようとするとき、ＤＲＭサーバは、どの識別サーバが識別証明書を交付したかを決定することができ、それにより、識別証明書を交付した識別サーバを信用するかどうかを決定することができる。先に論じたように、ＤＲＭサーバ３２０は、その信用する識別サーバのリストを調べることによってこの決定を行う。図１２には、２つの代替例リスト１２１２および１２１４が示してある。（ＤＲＭサーバ３２０が２つの信用リストを同時に使用することが必要なのではなく、これらのリストは、ＤＲＭサーバ３２０が使用できるリストの代替例として共に図１２に示すものである。）

【００８１】

リスト１２１２が使用される第１の例では、ＤＲＭサーバ３２０は、高セキュリティの識別サーバ１２０４は信用するが（このサーバの公開鍵証明書（ＰＵ－ＩＳ２）が信用リスト１２１２上にあるため）、ｅメールアドレスに基づくサーバ１２０２はどんな状況下でも信用しない。

【００８２】

リスト１２１４が使用される第２の例では、ＤＲＭサーバ３２０は、高セキュリティの識別サーバ１２０４を信用し、およびｅメールアドレスに基づく識別サーバ１２０２もいくつかの除外付きで信用する。例示的なリスト１２１４では、ｅメールに基づく公用の識別サーバ１２０２の信用は、特定の識別（ｊｏｅ@ｕｎｔｒａｃｅａｂｌｅａｄｄｒｅｓｓ．ｃｏｍ）または特定のドメイン名（ドメイン名ｈｉｇｈ－ｓｅｃｕｒｉｔｙ．ｃｏｍを有するすべてのアドレス）に交付された証明書を除外する。例えば、ｊｏｅ@ｕｎｔｒａｃｅａｂｌｅａｄｄｒｅｓｓ．ｃｏｍは、コンテンツ泥棒として知られている人物（例えばＤＲＭサーバ３２０を運営する会社の元従業員で不満を持っている者）であり、そのためＤＲＭサーバ３２０は彼を信用しない。ドメイン名全体を除外したいと思う場合の理由は、いくぶん反直感的である。高セキュリティのサーバ１２０４が、会社の識別サーバであり、ＸＸＸ@ｈｉｇｈ－Ｓｅｃｕｒｉｔｙ．ｃｏｍの形の識別を従業員に交付すると仮定する。会社は、自社の従業員を信用するが、従業員が会社の識別サーバ１２０４から得た識別証明書を実際に使用する場合にだけ従業員を信用したいことがある（このサーバはより強い認証プロシージャまたは会社ポリシー施行機能を有するので）。会社は、（より弱いセキュリティの）サーバ１２０２を介して自分を識別したい従業員がいれば、その従業員は会社の何らかのポリシーを回避しようとしていると推定することができる。ｈｉｇｈ－Ｓｅｃｕｒｉｔｙ．ｃｏｍを除外リストに載せることにより、高セキュリティのサー

バ１２０４を介して識別を得ることのできる人々はそのようにできることが保証され、また他の人々はｅメールアドレスに基づくサーバ１２０２を使用して自分を証明することができる。

【００８３】

図１２および前の考察では、ｅメールに基づく公用の識別サーバに関して除外リストを使用することについて説明したが、除外リストの概念は、任意の識別サーバに適用することができることを理解されたい。例えば、会社１のＤＲＭサーバは、会社２の識別サーバによって交付された識別を信用するが、会社１は、自社の従業員には自社のサーバを介して識別を得るようにさせたい。このため会社１のＤＲＭサーバは、会社２の識別サーバについての除外リストを維持することができ、それにより、会社２の識別サーバによって交付される証明書だが×××@ｃｏｍＰａｎｙ１．ｃｏｍの形のｅメールアドレスを指定する証明書があれば、この証明書はこの信用から除外される（会社１の従業員がドメインｃｏｍＰａｎｙ１．ｃｏｍ中のｅメールアドレスを有すると仮定した場合）。

【００８４】

別のサーバの権利ラベルに基づくライセンス交付

前述のように、ユーザは一般に、ライセンスの基づく権利ラベルに署名したＤＲＭサーバと同じＤＲＭサーバからライセンスを得る。この理由の１つには、ライセンスはコンテンツ鍵（ＣＫ）を含まなければならないが、コンテンツ鍵はＤＲＭサーバの公開鍵ＰＵ－ＤＲＭで暗号化されてライセンス中に記憶されるということがある。したがって、対応する秘密鍵ＰＲ－ＤＲＭを保有するＤＲＭサーバだけが、ライセンスを生み出すために鍵ＣＫを得ることができる。（一実施形態では、対称鍵ＤＥＳ１が使用され、それにより署名済み権利ラベルはＤＥＳ１（ＣＫ）およびＰＵ－ＤＲＭ（ＤＥＳ１）を含む。ただしこの効果は同じであり、ＣＫは、ＰＲ－ＤＲＭを保有する識別によってしか回復することができない。）しかし、あるＤＲＭサーバが、別のＤＲＭサーバによって発行された１つのコンテンツに対してライセンスを交付できることが望ましい場合がある。

【００８５】

このようなコンテンツの「相互ライセンス供与」を可能にする１つの方法は、第１のサーバ（コンテンツを発行したサーバ）が、その秘密鍵を別のサーバ（コンテンツをライセンス供与するサーバ）に提供するものである。秘密鍵を共有する際には注意を払わなければならない。ＤＲＭサーバの信用はその秘密鍵で表され、秘密鍵を有するものは誰でも、そのＤＲＭサーバに「扮する」（すなわち権利ラベルに署名しライセンスを交付する）ことができる。このため、第１のＤＲＭサーバの秘密鍵は、第２のＤＲＭサーバが秘密鍵を損ねることがないと確定できる場合にだけ、第２のＤＲＭサーバと共有すべきである。さらに、秘密鍵の移送は、移送中にうっかり誰かに漏れることがないように何らかの安全なスキームで行うことが好ましい。

【００８６】

図１３に、２つのＤＲＭサーバの例と、どのようにして一方のＤＲＭサーバを使用して他方のＤＲＭサーバによって交付された権利ラベルに基づくライセンスを交付することができるかを示す。ＤＲＭサーバ１（参照番号１３２０）は、鍵の対ＰＵ－ＤＲＭ１／ＰＲ－ＤＲＭ１を有し、ＤＲＭサーバ２（参照番号１３２２）は、鍵の対ＰＵ－ＤＲＭ２／ＰＲ－ＤＲＭ２を有する。ユーザ１３０２は、暗号化済みコンテンツ１３０４と、このコンテンツについての署名済み権利ラベル１３０６とを有する。ユーザ１３０２は、このコンテンツに対するライセンスを得たいと思っている。署名済み権利ラベルは、暗号化された形のコンテンツ鍵ＣＫを含み、したがってＣＫは、ＰＲ－ＤＲＭ１を使用して対称鍵ＤＥＳ１を復号してからＤＥＳ１をＤＥＳ１（ＣＫ）に適用してＣＫを得ることによってのみ、得ることが可能である。言い換えれば、ＰＲ－ＤＲＭ１がなければ、コンテンツ１３０４に対するライセンスを交付するためにＣＫを得ることは不可能である。このため、ユーザ１３０２が署名済み権利ラベル１３０６をＤＲＭサーバ２に送っても、このＤＲＭサーバは、コンテンツ１３０６に対するライセンスを交付することはできない。

【００８７】

しかし、ＤＲＭサーバ１がその秘密鍵ＰＲ－ＤＲＭ１をＤＲＭサーバ２と共有する場合（ＤＲＭサーバ１とＤＲＭサーバ２を結ぶ点線で表す）、ＤＲＭサーバ２は、この秘密鍵を使用してＣＫを入手し、ライセンスを交付することができる。

【００８８】

図１３には、ＰＲ－ＤＲＭ１をＤＲＭサーバ１からＤＲＭサーバ２に移送する例示的な方法の１つが示してある。図１３の例では、ＰＲ－ＤＲＭ１がＤＲＭサーバ２の公開鍵で暗号化されて、ＰＵ－ＤＲＭ２（ＰＲ－ＤＲＭ１）が生み出されている。これによりＰＲ－ＤＲＭ１は、公衆の目から保護され、ＰＵ－ＤＲＭ２（ＰＲ－ＤＲＭ１）をＤＲＭサーバ２の秘密鍵ＰＲ－ＤＲＭ２で復号することによって回復することができる。秘密鍵を移送する安全な方法は他にもあり、図１３に示す方法は例に過ぎないことを理解されたい。別の例としては、秘密鍵をディスクに収めて、信用される配達機関によって移送することができる。ＤＲＭサーバがアクセスできる秘密鍵のセットは、サーバの「信用文書領域」を定義する。

【００８９】

図１４に、このタイプの「相互ライセンス供与」スキームが有用な例を示す。会社１４００は、地理的に異なる場所に散在している。部門Ａ１４０２はアリゾナ州ウィンスローにあり、部門Ｂ１４０４はニュージャージー州アズベリーパークにある。実務上の理由で、各部門はそれぞれ、それ自体のＤＲＭサーバ１４０６および１４０８を維持している。例えば、これらの部門は、ＤＲＭサーバを使用して１日あたり何千もの文書を発行および／またはライセンス供与しており、これらの発行／ライセンス供与の業務すべてを実施するために国を横断してデータを移送することに依存するのは実行可能なことではない。しかし、部門ＡとＢは同じ会社１４００内にあるので、部門Ａの従業員は、部門Ｂの従業員にライセンス供与できるコンテンツを発行することができ、その逆も可能である。したがって、部門ＡとＢにいるユーザ１４１０と１４１２はそれぞれ、ＤＲＭサーバＡによって発行された何らかのコンテンツと、ＤＲＭサーバＢによって発行された何らかのコンテンツを有する。例えば、ユーザ１４１２は、ＤＲＭサーバＢ上で発行された何らかのコンテンツをユーザ１４１０に送り、ユーザ１４１０は、ＤＲＭサーバＡ上で発行された何らかのコンテンツをユーザ１４１２に送ることができる。

【００９０】

コンテンツの発行にどのサーバが使用されたかにかかわらず、各ユーザは、自分の部門にあるサーバに接触してライセンスを得る。したがって、ユーザ１４１０は、部門ＡのＤＲＭサーバ１４０６にライセンスを要求し、ユーザ１４１２は、部門Ｂのサーバ１４０８にライセンスを要求する。各サーバは、そのサーバが発行したどんなコンテンツに対してもライセンスを交付することができる。というのは、そのようなコンテンツについての権利ラベルは、そのサーバの公開鍵で生成されたものだからである。さらに、両サーバがそれぞれの秘密鍵ＰＲ－ＤＲＭＡおよびＰＲ－ＤＲＭＢを共有している限り、各サーバは、他方のサーバによって発行されたコンテンツに対するライセンスも交付することができる。

【００９１】

ライセンス要求に対する信用を妥当性検査するプロセス

図１５に、入来したライセンス要求に対する信用を妥当性検査するためにＤＲＭサーバが実施する例示的なプロセスを示す。このプロセスは以下の概念を含む。（１）識別証明書は、信用される識別サーバによって交付されなければならない。（２）ｅメールアドレスに基づく公用の識別サーバによって識別証明書が交付される場合、証明書中で指定されるペルソナ（例えばｊｏｅ@ｕｎｔｒａｃｅａｂｌｅａｄｄｒｅｓｓ．ｃｏｍ）またはドメイン（例えばｎｉｇｈ－ｓｅｃｕｒｉｔｙ．ｃｏｍ）は、除外リスト上にあってはならない。（３）権利ラベルは、ライセンス供与するＤＲＭサーバが関係を有するサーバによって交付されたものでなければならない。

【００９２】

ＤＲＭサーバは、入来したライセンス要求（署名済み権利ラベルおよび識別証明書を含むことが好ましい）を受け取った後、この識別証明書が「信用ペルソナ領域」にあるかどう

か、すなわち信用される識別サーバによって交付されたものかどうかを決定する（ステップ１５０２）。識別証明書が信用ペルソナ領域にない場合は、このライセンス要求は信用エラーにより拒否される（ステップ１５１２）。識別証明書が信用ペルソナ領域にある場合は、ステップ１５０４に進む。

【００９３】

ステップ１５０４で、ＤＲＭサーバは、この識別証明書を交付した信用される識別サーバに対して適用可能な除外リストがあるかどうかを決定する。前述の一例では、識別証明書の交付者は、ＭＩＣＲＯＳＯＦＴ．ＮＥＴ ＰＡＳＳＰＯＲＴサーバなどのｅメールアドレスに基づく公用の識別サーバであり、ＤＲＭサーバは、そのサーバによって交付された識別証明書が特定のｅメールアドレスおよび／またはドメインに交付されたものであれば、これらの識別証明書を異なるように扱うことを選択していた。ただし、除外リストは、信用ペルソナ領域中の任意の識別サーバに対して設定することができることを理解されたい。したがって、ステップ１５０４は一般に、特定の信用される識別サーバに関連する除外リストがあるかどうかを決定することを含む。

【００９４】

識別証明書を交付した識別サーバに関連する除外リストがない場合は、ステップ１５０８に進む。しかし、このような除外リストがある場合は、ＤＲＭサーバは、この証明書が交付されたペルソナに基づいて（例えばｅメールアドレス、ドメイン、または識別証明書中で指定されるその他の識別子に基づいて）、この識別証明書を除外すべきかどうか（すなわちこのような証明書に対してライセンスを拒否しなければならないかどうか）を決定する（ステップ１５０６）。このような理由で識別証明書を除外しなければならない場合は、このライセンス要求は信用エラーにより拒否される（ステップ１５１２）。一方、識別証明書を除外しなければならないと除外リストが指定しない場合は、ステップ１５０８に進む。

【００９５】

ステップ１５０８で、ＤＲＭサーバは、ライセンス要求中で提供される署名済み権利ラベルが、ライセンス供与するＤＲＭサーバの「信用文書領域」にあるＤＲＭサーバによって交付されたものかどうかを決定する。先に論じたように、この「信用文書領域」は、（ａ）ライセンス供与要求を処理しているＤＲＭサーバと、（ｂ）要求を処理しているＤＲＭサーバに秘密鍵を提供した（およびライセンス供与するＤＲＭサーバが信用し続ける）他のＤＲＭサーバとを含む。署名済み権利ラベルを交付したＤＲＭサーバが信用文書領域にない場合は、このライセンス供与要求は信用エラーにより拒否される（ステップ１５１２）。一方、署名済み権利ラベルが信用文書領域中のサーバによって交付されたものである場合は、信用要求の妥当性が認められ、ライセンス要求は処理される（ステップ１５１０）。

【００９６】

最終的なライセンス交付は、図５Ａ～５Ｂで先に説明したプロセスに従って行うことができる。さらに、図１５に説明したプロセスは、図５Ａ～５Ｂに説明したプロセスに追加するものとしてもよく、この２つのプロセスを共に織り交ぜてもよい。具体的には、ステップ１５０２、１５０４および１５０６は本質的に、要求側の識別を認証および許可する方法であり（図５Ａのステップ６０４および６０６に示すように）、ステップ１５０８は本質的に、署名済み権利ラベルを妥当性検査するための特定の方法である（図５Ｂのステップ６３０に示すように）。

【００９７】

結び

本発明に関連して実施されるプロセスを実現するのに必要なプログラミングは、比較的単純であり、関係するプログラミング界には明らかなはずである。したがって、このようなプログラミングは本明細書に添付しない。この場合、任意の具体的なプログラミングを採用して、本発明の趣旨および範囲を逸脱することなく本発明を実施することができる。

【００９８】

さらに、本発明の好適実施形態に多くの変更および修正を加えることができ、このような変更および修正は本発明の趣旨を逸脱することなく加えることができることは、当業者なら理解するであろう。したがって、特許請求の範囲は、本発明の真の趣旨および範囲に含まれるこのような等価な変形をすべてカバーするものとする。

【図面の簡単な説明】

【図１】本発明を実施することのできる例示的および非限定的なコンピューティング環境を表すブロック図である。

【図２】ディジタルコンテンツを発行するための、本発明によるシステムおよび方法の好適な実施形態の機能ブロック図である。

【図３】図３の方法によって生成された署名済み権利ラベルの構造を示すブロック図である。

【図４】権利管理されるディジタルコンテンツをライセンス供与するための、本発明によるシステムおよび方法の好適な実施形態の機能ブロック図である。

【図５Ａ】権利管理されるディジタルコンテンツをライセンス供与するための、本発明による方法の好適な実施形態のフローチャートである。

【図５Ｂ】権利管理されるディジタルコンテンツをライセンス供与するための、本発明による方法の好適な実施形態のフローチャートである。

【図６】本発明の特徴による権利管理システムをサポートする暗号機能を有するプラットフォームのブロック図である。

【図７】本発明の態様による例示的な識別証明書のブロック図である。

【図８】本発明の態様による例示的なライセンスのブロック図である。

【図９】鍵保護層の間の関係、および信用のチェインを示すブロック図である。

【図１０】本発明の態様による、識別サーバの選択的な信用を示すブロック図である。

【図１１】２つの組織間で文書を共有することを可能にする信用ペルソナ領域の例示的な使用法のブロック図である。

【図１２】本発明の態様による、ｅメールに基づく公用の識別サーバを含む例示的なアーキテクチャのブロック図である。

【図１３】本発明の態様による、第１のＤＲＭサーバが別のＤＲＭサーバに代わってコンテンツをライセンス供与できるようにするために秘密鍵を共有することを示すブロック図である。

【図１４】２つの会社部門の間で保護コンテンツを相互ライセンス供与することを可能にする信用文書領域の例示的な使用法のブロック図である。

【図１５】本発明の態様による、ライセンス要求に対する信用を妥当性検査する例示的なプロセスを示す流れ図である。

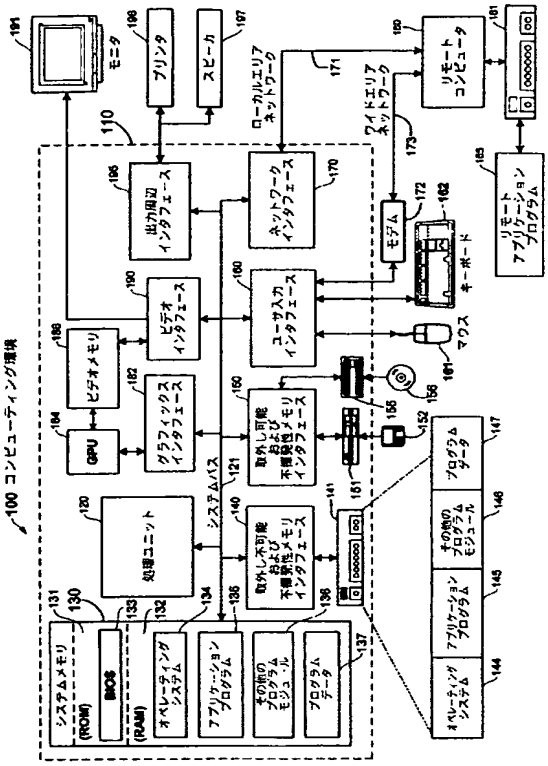
【符号の説明】

１００　コンピューティング環境
１１０　コンピュータ
１２０　処理ユニット
１２１　システムバス
１３０　システムメモリ
１３１　ＲＯＭ
１３２　ＲＡＭ
１３３　ＢＩＯＳ
１３４　オペレーティングシステム
１３５　アプリケーションプログラム
１３６　その他のプログラムモジュール
１３７　プログラムデータ
１４０　取外し不可能および不揮発性メモリインタフェース
１４１　ハードディスクドライブ
１４４　オペレーティングシステム

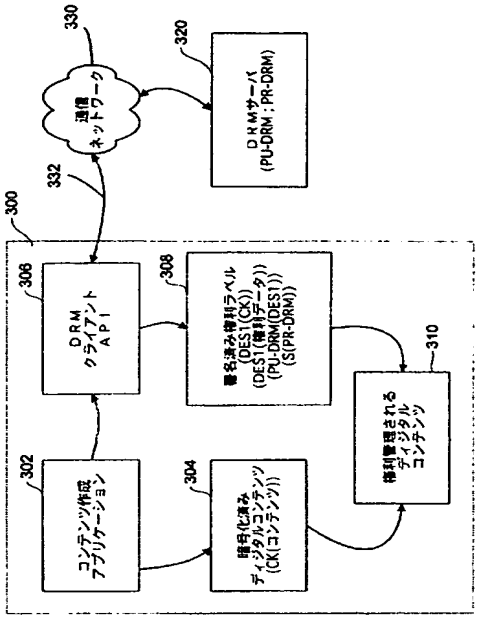
１４５　アプリケーションプログラム
１４６　その他のプログラムモジュール
１４７　プログラムデータ
１５０　取外し可能および不揮発性メモリインタフェース
１５１　磁気ディスクドライブ
１５２　磁気ディスク
１５５　光ディスクドライブ
１５６　光ディスク
１６０　ユーザ入力インタフェース
１６１　ポインティングデバイス
１６２　キーボード
１７０　ネットワークインタフェース
１７１　ローカルエリアネットワーク（ＬＡＮ）
１７２　モデム
１７３　ワイドエリアネットワーク（ＷＡＮ）
１８０　リモートコンピュータ
１８１　メモリ記憶デバイス
１８２　グラフィックスインタフェース
１８４　グラフィックス処理ユニット（ＧＰＵ）
１８５　リモートアプリケーションプログラム
１８６　ビデオメモリ
１９０　ビデオインタフェース
１９１　モニタ
１９５　出力周辺インタフェース
１９６　プリンタ
１９７　スピーカ
３００　クライアント
３０２　コンテンツ作成アプリケーション
３０２　クライアントアプリケーション
３０４　暗号化済みディジタルコンテンツ
３０６　ＤＲＭクライアントＡＰＩ
３０８　署名済み権利ラベル（ＳＲＬ）
３１０　権利管理されるディジタルコンテンツ
３１２　復号されたディジタルコンテンツ
３２０　ＤＲＭサーバ
３３０　通信ネットワーク
６０２　プラットフォーム
６０４　暗号モジュール
７０２　識別証明書
８０２　ライセンス
９０２　コンテンツ
９０４　コンテンツ鍵
９０６　エンティティ鍵の対
９０８　プラットフォーム鍵の対
９１２　コンテンツ所有者
９１４　ライセンス供与側
９１６　エンティティ証明書交付者
９１８　プラットフォーム
１００２（１）　識別サーバ１
１００２（２）　識別サーバ２

１００４（１）　識別証明書１
１００４（２）　識別証明書２
１１０２　会社Ａの識別サーバ
１１０４　会社Ｂの識別サーバ
１１０６　会社ＡのＤＲＭサーバ
１１０８　会社ＢのＤＲＭサーバ
１１１０　信用される識別サーバのリスト
１１１２　信用される識別サーバのリスト
１２０２　識別サーバ
１２０４　高セキュリティの識別サーバ
１２０６　プラットフォーム１
１２０８　プラットフォーム２
１２１０　ライセンス要求
１２１２　信用される識別サーバのリスト
１２１４　信用される識別サーバのリスト
１３２０　ＤＲＭサーバ１
１３２２　ＤＲＭサーバ２
１３０２　ユーザ
１３０４　暗号化済みコンテンツ
１３０６　署名済み権利ラベル
１４０２　部門Ａ
１４０４　部門Ｂ
１４０６　ＤＲＭサーバＡ
１４０８　ＤＲＭサーバＢ
１４１０　部門Ａのユーザ
１４１２　部門Ｂのユーザ

【図１】



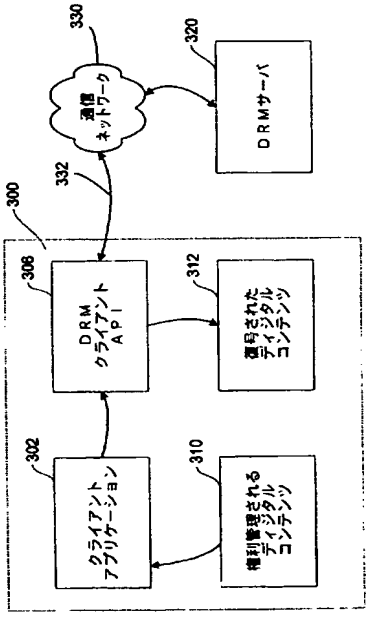
【図２】



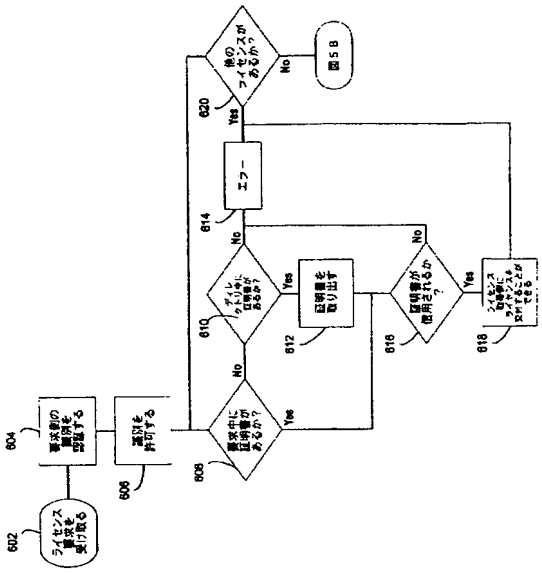
【図３】

SRL 308
コンテンツ情報
ＤＲＭサーバ情報
- (PU-DRM(DES1))
- 参照情報
- - URL
- -フォールバック
権利ラベル情報
(DES1(権利データ))
(DES1(CK))
S (PR-DRM)

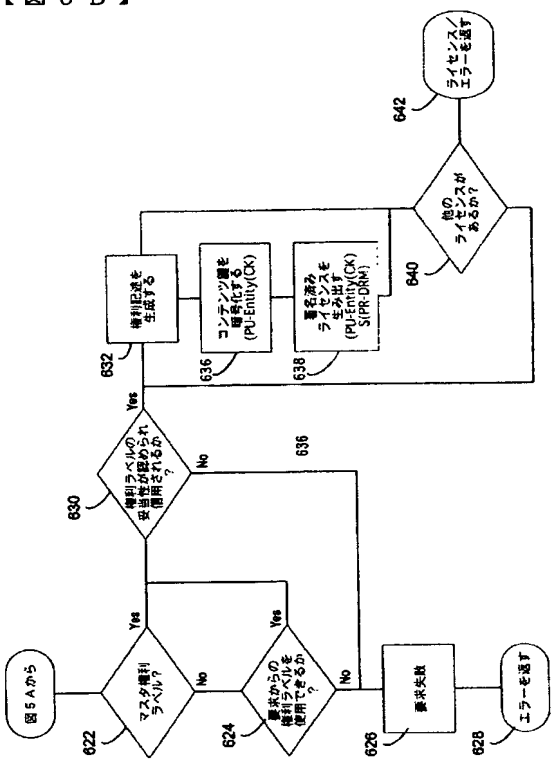
【図４】



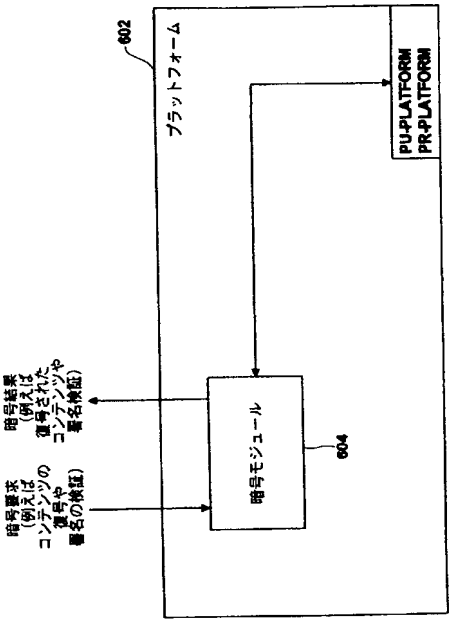
【図５Ａ】



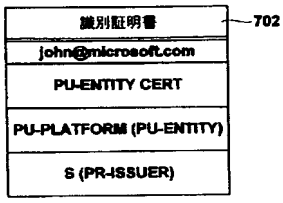
【図５Ｂ】



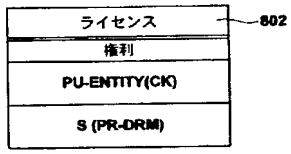
【図６】



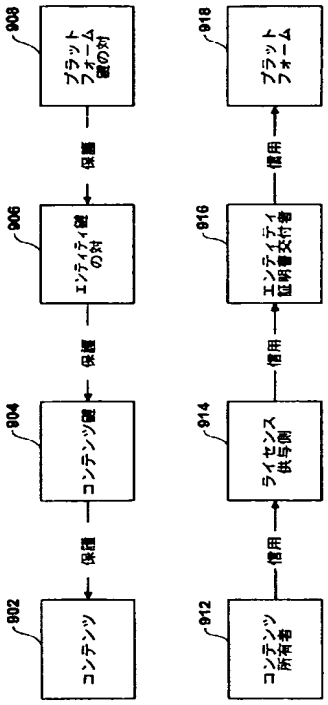
【図７】



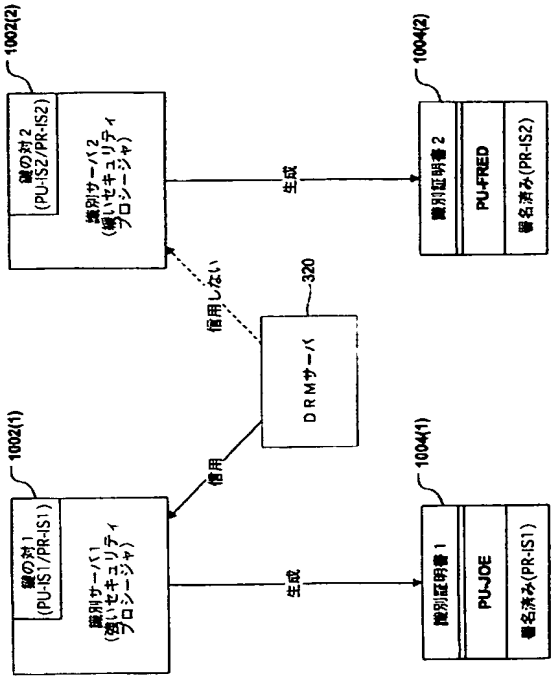
【図８】



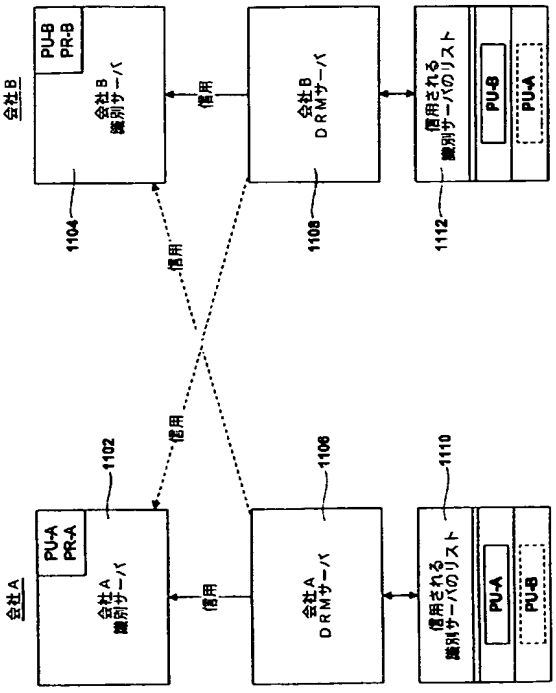
【図９】



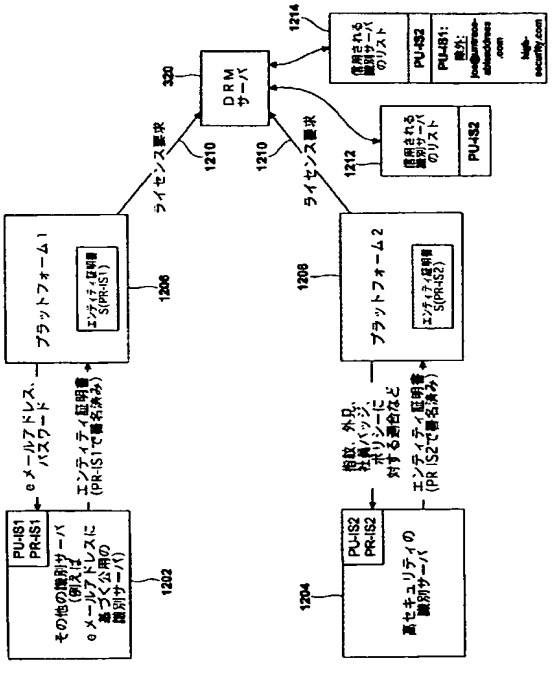
【図１０】



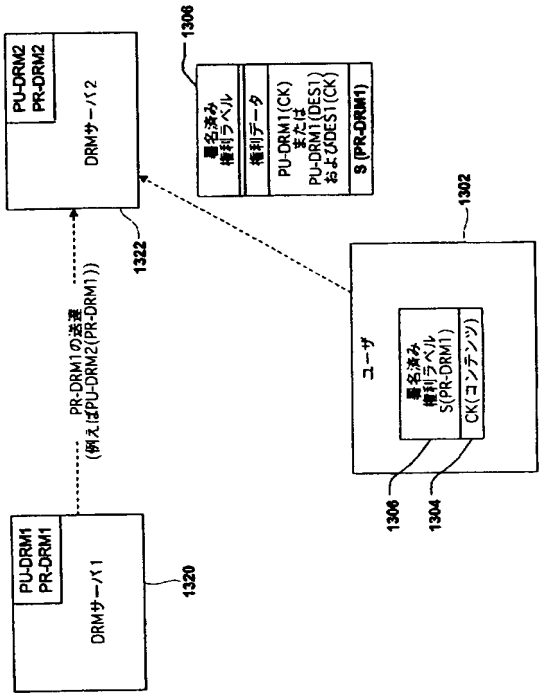
【図１１】



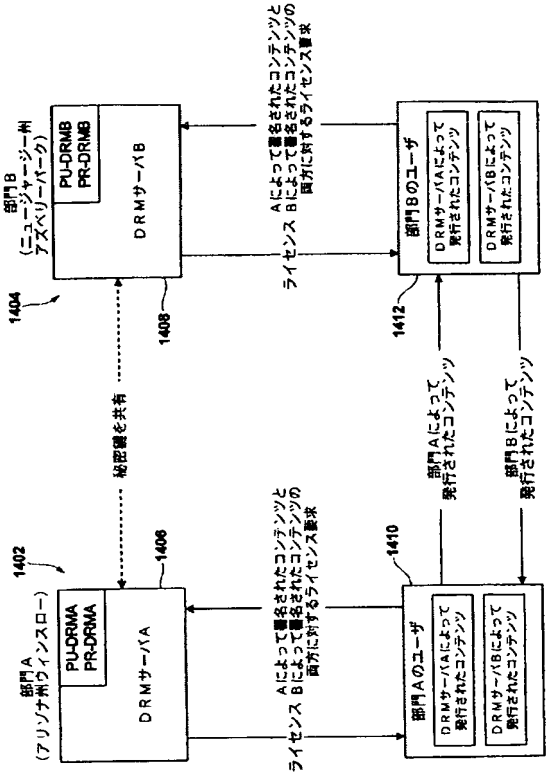
【図１２】



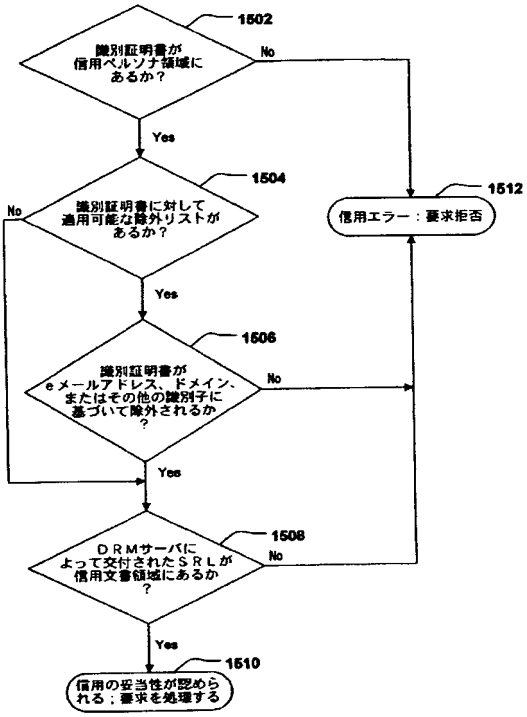
【図１３】


PU-DRM2
PR-DRM2
DRMサーバ2
1322
1306
署名済み
権利ラベル
権利データ
PU-DRM1(CK)
または
PU-DRM1(DES1)
およびDES1(CK)
S(PR-DRM1)
1302
ユーザ
署名済み
権利ラベル
S(PR-DRM1)
CK(コンテンツ)
1306
1304
PR-DRM1の送達
(例えばPU-DRM2(PR-DRM1))
PU-DRM1
PR-DRM1
DRMサーバ1
1320

【図１４】


部門B
(ニュージャージー州
アズベリーパーク)
PU-DRMB
PR-DRMB
DRMサーバB
1404
1408
Aによって署名されたコンテンツと
Bによって署名されたコンテンツの
両方に対するライセンス要求
ライセンス
部門Bのユーザ
DRMサーバAによって
発行されたコンテンツ
DRMサーバBによって
発行されたコンテンツ
1412
秘密鍵を共有
部門A
(アリゾナ州ウィンスロー)
PU-DRMA
PR-DRMA
DRMサーバA
1402
1406
Aによって署名されたコンテンツと
Bによって署名されたコンテンツの
両方に対するライセンス要求
ライセンス
部門Aのユーザ
DRMサーバAによって
発行されたコンテンツ
DRMサーバBによって
発行されたコンテンツ
1410
部門Aによって
発行されたコンテンツ
部門Bによって
発行されたコンテンツ

【図１５】


1502
識別証明書が
信用ペルソナ領域に
あるか？
No
Yes
1504
識別証明書に対して
適用可能な除外リストが
あるか？
No
Yes
1506
識別証明書が
eメールアドレス、ドメイン、
またはその他の識別子に
基づいて除外されるか
？
No
Yes
1508
DRMサーバに
よって交付されたSRLが
信用文書領域にあるか
？
No
Yes
1512
信用エラー：要求拒否
1510
信用の妥当性が認められる；要求を処理する

フロントページの続き

(51)Int.Cl.[7]	FI		テーマコード（参考）
	G06F 17/60	ZEC	
	H04L 9/00	601F	
	H04L 9/00	601B	

(72)発明者 ピーター デビッド ワックスマン
アメリカ合衆国 98004 ワシントン州 ベルビュー ノースイースト 28 プレイス 10008
(72)発明者 トーマス ケー. リンデマン
アメリカ合衆国 98052 ワシントン州 レッドモンド ノースイースト 133 プレイス 17225
(72)発明者 フランク バイラム
アメリカ合衆国 98101 ワシントン州 シアトル ウエスタン アベニュー 1200 ナンバー1210

Fターム(参考) 5B017 AA07 BA06 BA07 CA16
5B085 AE09 AE23 AE29 BG01 BG04 BG07
5J104 EA05 EA17 EA19 PA10